إنترنت الأجسام

الفرص، المخاطر، الحوكمة

ماري لي (MARY LEE) | بنجامين بودرو (BENJAMIN BOUDREAUX) | ريتيكا شاتورفيدي (RITIKA CHATURVEDI)
ساشا رومانوسكي (SASHA ROMANOSKY) | برايس دونينج (BRYCE DOWNING)



تصميم الغلاف: بيتر سوريانو *(Peter Soriano)*
صورة الغلاف: أدوبي ستوك *(Adobe Stock)*/أنطوني آرت *(anttoniart)*

للمزيد من المعلومات حول هذا المنشور، الرجاء زيارة الموقع الإلكتروني:
www.rand.org/t/RR3226

ما هو إنترنت الأجسام (Internet of Bodies)؟

تَعِد حالياً مجموعةٌ كبيرةٌ من الأجهزة "الذكيّة" المتّصلة بالإنترنت المُستهلِكين وشركات الأعمال بتحسين الأداء، والملاءمة، والفعاليّة، والمرح. فضمن نطاق إنترنت الأشياء (Internet of Things [IoT]) هذا الأوسع، تكمن صناعةٌ متناميةٌ لأجهزةٍ تَرْصُد الجسم البشريّ، وتجمع معلوماتٍ صحيّةً وشخصيّةً أخرى، وتنقل تلك البيانات عبْر الإنترنت. إنّنا نشير إلى هذه التكنولوجيات الناشئة والبيانات التي تَجْمَعها بمصطلح إنترنت الأجسام (*Internet of Bodies* [IoB]) (راجِع مثلاً، نيل [Neal]، 2014؛ لي [Lee]، 2018)، وهو مصطلح طبّقته أوّلاً البروفيسورة في مجال القانون والهندسة أندريا م. ماتويشين (Andrea M. Matwyshyn) على مجال القانون والسياسات عام 2016 (المجلس الأطلسي [Atlantic Council]، 2017؛ ماتويشين [Matwyshyn]، 2016؛ ماتويشين [Matwyshyn]، 2018؛ ماتويشين [Matwyshyn]، 2019).

تأتي أجهزة إنترنت الأجسام في أشكالٍ متعدّدة. يُستخدَم بعضها أصلاً على نطاقٍ واسع، مثل أجهزة رصْد اللياقة البدنية المُضمَّنَة في ساعات اليد أو مُنَظِّمات ضربات القلب التي تنقل بيانات حول قلب مريضٍ ما مباشرةً إلى طبيب القلب. وقد تكون منتجات أخرى، والتي هي قيد التطوير أو مطروحة حديثاً في السوق، أقلّ شعبيّةً مثل المنتجات القابِلة للهضم التي تجمع معلومات حول أمعاء شخصٍ ما وترسلها، والرقاقات الدقيقة المزروعة في الجسم، وأجهزة تحفيز الدماغ، والمراحيض المتّصلة بالإنترنت.

إنّ لهذه الأجهزة وصولٌ وثيقٌ إلى الجسم وهي تجمع كميّاتٍ هائلةً من البيانات البيومتريّة الشخصيّة. تَعِد الجهات المُصنِّعَة لأجهزة إنترنت الأجسام بتوفير منافع صحيّة وأخرى كبيرة ولكنّها تُشكّل أيضاً مخاطر كبيرة، بما فيها مخاطر التخريب (القرصنة) الإلكتروني، أو انتهاكات الخصوصية، أو العطل. وقد يُحدِث بعض الأجهزة، مثل بنكرياس اصطناعي موثوق لمرضى داء السكري، ثورةً في علاج المرض، في حين كل ما يمكن أن تفعله أجهزة أخرى هو تضخيم تكاليف الرعاية الصحيّة ويكون لها تأثير إيجابي محدود على النتائج. قد يُحدِث الوصول إلى كميات ضخمة من المعلومات البيومتريّة المباشرة البثّ إنجازات في مجال المعرفة الطبيّة أو الفهْم السلوكيّ. وقد يزيد من التباينات على مستوى النتائج الصحيّة، حيث لا يصل إلى أيٍّ من هذه المنافع إلا الأشخاص الميسورون. أو أنّه قد يُمكِّن أيضاً دولةً تعتمد المراقَبَة الجماعية (surveillance state) وقادرة على تحقيق اختراقٍ ونتيجةٍ غير مسبوقيْن.

ما من تعريفٍ مقبولٍ عموماً لإنترنت الأجسام.[1] فلأغراض هذه الدراسة، إنّنا نشير إلى إنترنت الأجسام، أو النظام البيئي لإنترنت الأجسام، على أنّه أجهزة إنترنت الأجسام (*IoB devices*) (التي يتم تعريفها لاحقاً، مع تفسيرٍ إضافيٍّ في المقاطع التي تلي) بالإضافة إلى البرمجيات التي تَضُمُّها والبيانات التي تَجْمَعها.[2]

يتم تعريف جهاز إنترنت الأجسام على أنّه جهازٌ

الاختصارات

AI	artificial intelligence الذكاء الاصطناعي
CCPA	California Consumer Privacy Act قانون كاليفورنيا لحماية خصوصية المستهلِك
CFIUS	Committee on Foreign Investment in the United States لجنة الاستثمار الأجنبي في الولايات المتحدة
CGM	continuous glucose monitor جهاز الرصد المستمرّ لمستوى الجلوكوز في الدمّ
CPAP	continuous positive airway pressure الضغط الإيجابي المستمرّ في المجرى الهوائي
EHR	electronic health record السجلّ الصحّيّ الإلكترونيّ
EU	European Union الاتحاد الأوروبيّ
EULA	end user license agreement اتفاقية ترخيص المستخدِم النهائي
FDA	U.S. Food and Drug Administration إدارة الغذاء والدواء
FTC	Federal Trade Commission لجنة التجارة الفيدراليّة
GDPR	General Data Protection Regulation اللائحة التنظيمية العامة لحماية البيانات
H-ISAC	Health Information Sharing Analysis Center مركز تبادل المعلومات الصحيّة وتحليلها
HIPAA	Health Insurance Portability and Accountability Act قانون نقْل التأمين الصحي والمساءلة
ICS-CERT	Industrial Control Systems Cyber Emergency Readiness Team فريق الجهوزية للطوارئ الإلكترونية المتعلقة بأنظمة المراقبة الصناعيّة
IoB	Internet of Bodies إنترنت الأجسام
IoT	Internet of Things إنترنت الأشياء
MDIC	Medical Device Innovation Consortium اتّحاد ابتكار الأجهزة الطبيّة
NCD	noncommunicable disease المرض غير الساري
NFC	near-field communication الاتصال القريب المدى
NIST	National Institute of Standards and Technology المعهد الوطني للمعايير والتكنولوجيا
NITRD	Networking and Information Technology Research and Development برنامج البحث والتطوير في مجال إقامة الشبكات وتكنولوجيا المعلومات
PGHD	person-generated health data البيانات الصحيّة المولَّدة من الشخص
RFID	radio frequency identification التعرّف بالترددات اللاسلكيّة

- يضمّ برمجيّات أو قدرات حاسوبيّة
- يستطيع التواصل مع جهازٍ متّصلٍ بالإنترنت أو شبكة

ويفي بأحد الأمرين التاليين أو بكليهما معاً:

- يجمع البيانات الصحيّة المولَّدة من الشخص أو البيومتريّة
- يستطيع تغيير وظيفة الجسم البشريّ.

قد تكون البرمجيات أو القدرات الحاسوبيّة في جهازٍ لإنترنت الأجسام بسيطةً جداً بحيث تقتصر على بضعة أسطُرٍ من رمزٍ تُسْتَخْدَم لإعداد رقاقةٍ دقيقةٍ مزروعةٍ في الجسم للتعرّف بالتردّدات اللاسلكيّة (radio frequency identification [RFID])، أو معقّدةً جداً على شكل حاسوبٍ يُعالِج الذكاء الاصطناعي (artificial intelligence [AI]) وخوارزميّات التعلُّم الآلي (machine learning algorithms). يكون الاتّصال بالإنترنت من خلال الشبكات الخليويّة أو شبكات تقنية الاتصال اللاسلكي (الواي فاي) (Wi-Fi) مطلوباً بدون أن يكون بالضرورة اتصالاً مباشراً. فعلى سبيل المثال، يجوز أن يكون جهازٌ ما متّصلاً عبْر البلوتوث (Bluetooth) بهاتفٍ ذكيٍّ أو جهاز ناقلٍ تسلسليٍّ عامٍ (USB device) يتواصل مع حاسوبٍ متّصلٍ بالشبكة. وتشير البيانات الصحيّة المولَّدَة من الشخص *(person-generated health data [PGHD])* إلى البيانات الصحيّة، أو السريريّة أو المتعلّقة بالرفاهية والتي تَجْمَعها التكنولوجيّات ليتم تسجيلها أو تحليلها من قِبَل المستَخْدِم أو شخصٍ آخر. وتشير البيانات البيومترية أو السلوكيّة إلى قياسات الخصائص الجسديّة أو السلوكيّة الفريدة بشأن شخصٍ ما. وأخيراً، يشير "تغيير" لوظيفة الجسم إلى زيادةٍ أو تعديلٍ لكيفيّة أداء جسم المُسْتَخْدِم، مثل تغييرٍ في التعزيز المعرفيّ وتحسين الذاكرة توفّرهما واجهة دماغ وحاسوب (brain-computer interface)، أو القدرة على تسجيل أي شيء يراه المُستَخْدِم من خلال عدسة مزروعةٍ داخل العين (intraocular lens) ومزوَّدَة بكاميرا.

تتطلّب أجهزة إنترنت الأجسام عموماً، وإنما ليس دائماً، اتصالاً جسدياً بالجسم (مثلاً، يتم ارتداؤها، أو هضْمها، أو زرْعها أو وصْلها بخلاف ذلك بالجسم أو تضمينها فيه، إنْ بشكلٍ مؤقتٍ أو دائم). إنّ عدداً من أجهزة إنترنت الأجسام هو أجهزة طبيّة تخضع لتنظيم إدارة الغذاء والدواء (Food and Drug Administration [FDA]) الأمريكيّة.[3] ويصوِّر الشكل رقم 1 أمثلةً حول التكنولوجيات في النظام البيئي لإنترنت الأجسام والتي هي متوفّرة أصلاً في السوق الأمريكية أو قيد التطوير.

ليست الأجهزة غير المتّصلة بالإنترنت، مثْل أجهزة مراقبة القلب العاديّة (ordinary heart monitors) أو أساور تحديد الهوية الطبيّة (medical ID bracelets)، مشمولةً في تعريف إنترنت الأجسام. وليست مشمولةً أيضاً بالتعريف المغناطيسات المزروعة في الجسم (الطعوم المغناطيسيّة) (implanted magnets) (وهي مُنتَج استهلاكي متخصّص يستخدمه هؤلاء في ما يُدعى مجتمع القراصنة الإلكترونيين للأجسام [bodyhacker community]، الذي يرِد وصْفه في القسْم التالي) التي ليست متّصلة بتطبيقات الهواتف الذكيّة (التطبيقات [apps]) لأنّه، وعلى الرغم من أنّها تُغَيِّر وظيفة الجسم من خلال السماح للمُستَخْدِم باستشعار الاهتزازات الكهرومغناطيسيّة، لا تحتوي الأجهزة على برمجيات. ويَرِد مزيدٌ من مناقشة الاتّجاهات في تكنولوجيات إنترنت الأجسام وأمثلة إضافيّة في القسْم التالي.

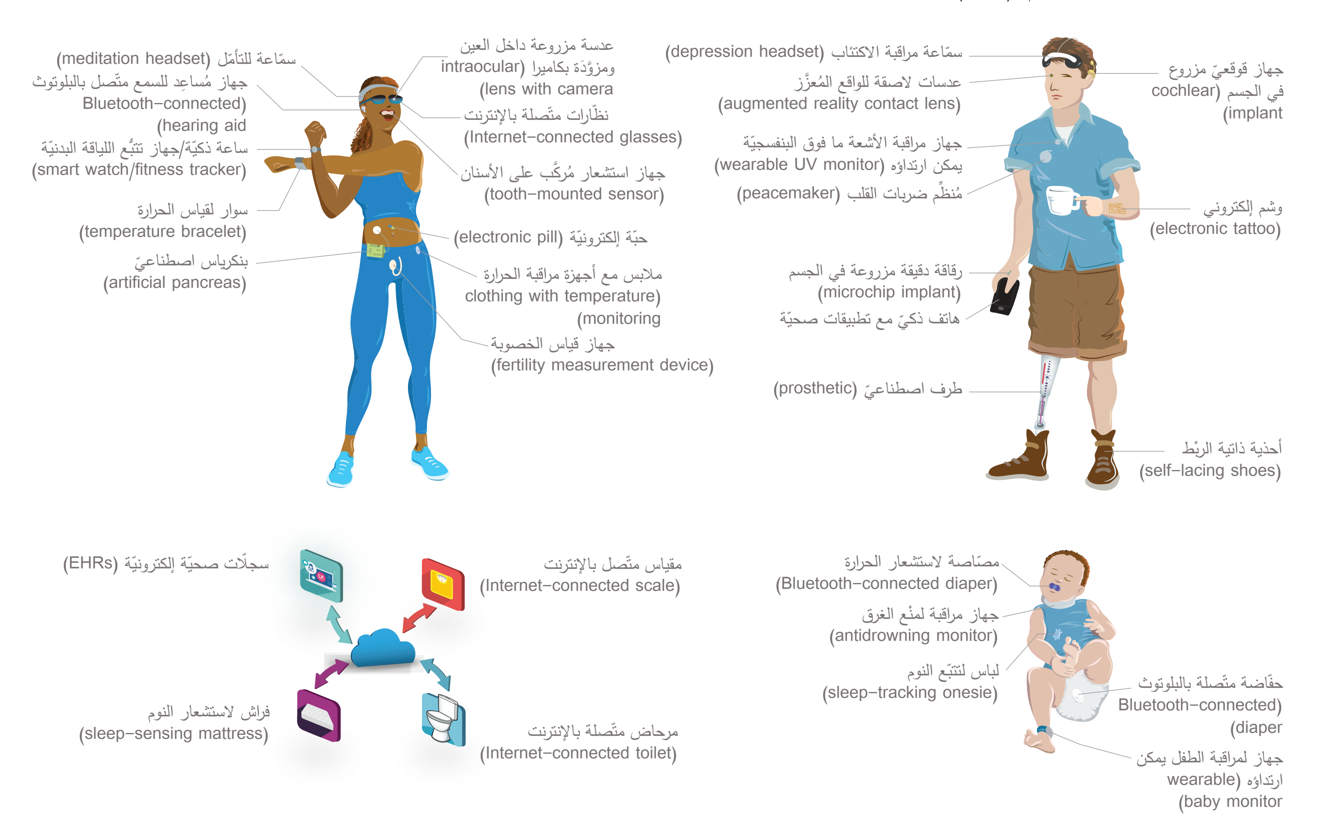
قد يندرج بعض أجهزة إنترنت الأجسام ضمن نطاق تعريفنا أو يخرج عنه في أوقاتٍ مختلفة. فعلى سبيل المثال، قد لا يكون هاتفٌ ذكيٌّ متّصلٌ بشبكة تقنية الاتصال اللاسلكي (الواي فاي) بحدّ ذاته جزءاً من إنترنت الأجسام؛ ولكن، ما أن يتم تنزيل تطبيق صحيّ عليه يتطلّب الاتصال بالجسم لتتبُّع معلومات المُستَخْدِم، مثل معدّل ضربات القلب أو عدد الخطوات التي يخطوها، قد يُعتَبَر الهاتف جهازاً لإنترنت الأجسام. يهدف تعريفنا إلى تحديد التكنولوجيات السريعة التطوّر التي تقترن بالقدرة على إحداث المخاطر والمنافع المختلفة التي تتم مناقشتها في هذه الدراسة. لقد ركّزنا على تحليل تكنولوجيات إنترنت الأجسام القائمة وتلك الناشئة التي يبدو أنّها تقترن بالقدرة على تحسين النتائج الصحيّة والطبيّة، والفعاليّة، والوظيفة أو الأداء البشريّ، وإنّما التي قد تُعَرِّض أيضاً حقوق المُستخدِمين القانونية، والأخلاقيّة وتلك المتعلّقة بالخصوصيّة للخطر أو قد تُشكّل مخاطر على الأمن الشخصيّ أو القومي.

لقد أجرينا لهذا البحث مراجعةً واسعة النطاق للدراسات السابقة وقابلنا خبراء أمنيين، ومطوِّرين تكنولوجيين، ومؤيّدين لإنترنت الأجسام من أجل فهْم المخاطر والمنافع المُتَوَقَّعَة. وأجرينا مناقشات قيّمة مع خبراء في المؤتمر حول القرصنة الأخلاقية للأجسام عام 2019 (BDYHAX 2019)، وهو مؤتمر سنويّ للقراصنة الإلكترونيين للأجسام عُقِد في فبراير/شباط 2019، وفي مؤتمر ديفكون 27 (DEFCON 27)، وهو أحد المؤتمرات الأكبر في العالَم للقراصنة الإلكترونيين، عُقِد في أغسطس/آب 2019. وإنّنا في هذه الدراسة نناقش الاتجاهات في مشهد التكنولوجيا ونحدّد المنافع والمخاطر بالنسبة إلى المسْتَخْدِم وأصحاب الشأن الآخرين. ونعرض حالة الحوكمة الحاليّة التي تنطبق على أجهزة إنترنت الأجسام والبيانات التي تجمعها ونختم بتقديم توصيات لتحسين التنظيم من أجل تحقيق التوازن الأفضل بين تلك المخاطر والفوائد.

مشهدٌ ناشئٌ للأجهزة والأفكار

إنترنت الأشياء (Internet of Things)

يرتبط إنترنت الأجسام (IoB) ارتباطاً وثيقاً بإنترنت الأشياء (IoT)،[4] والذي ما مِنْ تعريفٍ عام له أيضاً؛ على الرغم من ذلك، لأجهزة إنترنت الأشياء خصائص متعدّدة متّفق عليها على نطاقٍ واسع. أوّلاً، تكون أجهزة إنترنت الأشياء متّصلةً بالإنترنت إمّا مباشرةً أو من خلال شبكةٍ محليّة. ثانياً، يكون لها على الأقلّ واحدة من الوظائف التالية: القدرة على إحداث بعضٍ من التغيير الجسدي أو استشعاره، أو الحصول مباشرةً على معلوماتٍ من البشر أو



الشكل رقم 1
أمثلة حول إنترنت الأجسام (IoB)

تقديم المعلومات لهم، أو استعادة البيانات أو تخزينها. وأخيراً، يجب أن تتفاعل أجهزة إنترنت الأشياء من أجل توفير بعض المنافع للمُستَخْدِم. فمثلاً، يمكن برمجة مصباحٍ كهربائيٍّ ما ليشتغل عند الغسق بدون أن يكون متّصلاً بشبكةٍ ما. وهو لا يصبح جزءاً من إنترنت الأشياء إلّا عندما يتم وصْله بجهاز إنترنت أشياء آخر، مثل هاتفٍ ذكيّ، ما يتيح عندئذٍ لمُستَخْدِمٍ ما تشغيل الضوء بدون أن يكون متواجداً في المنزل. فانطلاقاً من تعريفاتنا، يُعتبر أي واحد من أجهزة إنترنت الأجسام جهاز إنترنت أشياء.

يشمل تعريفنا لإنترنت الأجسام التكنولوجيات الناشئة ممّا يُدعى إنترنت الأشياء للرعاية الصحيّة *(health-care Internet of Things)* (هيلي [Healey]، بولارد [Pollard]، وودز [Woods]، 2015)، على الرغم من أنّ أجهزة إنترنت الأشياء للرعاية الصحيّة قد لا تُعتبر جميعها أجهزةً لإنترنت الأجسام. تُعتبر السجلات الصحيّة الإلكترونية (EHRs)، والأنظمة الجراحيّة الروبوتيّة، والأجهزة المُستَخْدَمَة للعلاج الطبي، مثْل أجهزة التنفّس الاصطناعي الذكيّة، جميعها جزءاً من النظام البيئي لإنترنت الأجسام لأنّها تجمع معلومات حول المُستَخْدِمين أو تُغَيِّر وظيفة الجسم. على الرغم من ذلك، فإن البرّاد "الذكي" في مستشفى ما، المُستَخْدَم لتخزين اللقاحات والذي يمكن وصْله بشبكةٍ ويُنْذِر فريق العمل في حال تدنّي المخزون، لا يعتبر جهازاً لإنترنت الأجسام لأنّه لا يتوافق مع تعريفنا.

حركة ما بعْد الإنسانيّة (Transhumanism)، والقرصنة الإلكترونيّة للأجسام (Bodyhacking)، والقرصنة الإلكترونيّة البيولوجيّة الأخلاقيّة (Biohacking) وغيرها

يرتبط إنترنت الأجسام (IoB) بحركات متعدّدة خارج نطاق الرعاية الصحيّة الرسميّة والتي تركّز على دمْج الأجسام البشريّة مع التكنولوجيا. إنّنا نلخّص تالياً بعض هذه المفاهيم،[5] على الرغم من وجود الكثير من التداخل والتبادل بينها.

ما بعْد الإنسانيّة *(transhumanism)* هي نظرة عالميّة وحركة سياسيّة تؤيّد تجاوز الإنسانيّة للقدرات البشريّة الحاليّة. يريد أتباع حركة ما بعْد الإنسانيّة استخدام التكنولوجيا، على غرار الأعضاء الاصطناعيّة والتقنيات الأخرى، لوقْف الشيخوخة وتحقيق "إطالة الحياة الجذرية" (فيتا-مور [Vita-Moore]، 2018). وقد يسعى أتباع حركة ما بعْد الإنسانيّة أيضاً وراء مقاومة المرض، أو تعزيز ذكائهم، أو إحباط التعب من خلال النظام الغذائي، أو التمرين الرياضي، أو المغذيات التكميلية، أو تقنيات الاسترخاء أو المنشّطات العقليّة-الدماغيّة (nootropics) (وهي مواد قد تحسِّن الوظيفة المعرفيّة).

غالباً ما يشير القراصنة الإلكترونيون للأجسام، والقراصنة الإلكترونيون البيولوجيون الأخلاقيون، والسايبورغات أي المتعضات السيبرناطيقية (وهي كائنات نظرية أو خيالية تتكون من مزيج من

مكونات عضوية وبيو–ميكاترونية)، والذين يستمتعون باختبار تعزيز الجسم، إلى أنفسهم بمصطلح الطواحِن *(grinders)*. فقد يجوز أو لا يجوز تحديدهم على أنّهم من أتباع حركة ما بعْد الإنسانيّة. غالباً ما يتم التبديل بين هذه المصطلحات في الاستخدام الشائع، إلّا أنّ البعض يميّز فيما بينها (ترامِل [Trammell]، 2015). تشير عموماً القرصنة الإلكترونيّة للأجسام *(bodyhacking)* إلى تعديل الجسم من أجل تعزيز القدرات الجسدية أو المعرفية لدى شخصٍ ما. يُعتَبَر بعض أنشطة القرصنة الإلكترونيّة للأجسام تجميلياً بحتاً. فقد زرَع القراصنة الإلكترونيون أبواقاً في رؤوسهم وأضواء ليد (LED) تحت جلدهم. وتهدف عمليات قرصنة إلكترونيّة أخرى، مثل زرْع الرقاقات الدقيقة للتعرّف بالترددات اللاسلكيّة (RFID) في يد شخصٍ ما، إلى تعزيز الوظيفة، ما يتيح للمُستَخدِمين فتْح قفْل الأبواب، أو ركوب وسائل النقل العامّة، أو تخزين معلومات الاتصال في حالات الطوارئ، أو إتمام عمليات الشراء بحركة بسيطة (بينين [Baenen]، 2017؛ سافاج [Savage]، 2018). وقد نَزَعَت إحدى القراصنة الإلكترونيين للأجسام الرقاقة الدقيقة للتعرّف بالترددات اللاسلكيّة من نظام مفاتيح سيّارتها وتمّ زرْعها في ذراعها (ليندِر [Linder]، 2019). وزرَع بعض القراصنة الإلكترونيين للأجسام جهازاً هو كناية عن موجِّهٍ لاسلكيّ (wireless router) وقرصٍ صلب (hard drive) والذي يمكن استخدامه بمثابة عقدةٍ في شبكةٍ متداخلةٍ لاسلكيّة (أوبرهوس [Oberhaus]، 2019). ويُعتَبَر بعض أنشطة القرصنة الإلكترونية للأجسام طبّياً بطبيعته، بما في ذلك الأعضاء الاصطناعية المطبوعة بتقنيةٍ ثلاثية الأبعاد والبنكرياسات الاصطناعية المُصمَّمَة للهواة. ومع ذلك يستخدم البعض المصطلح للإشارة إلى أيّ أسلوبٍ معتمدٍ لتحسين الصحّة، بما في ذلك كمال الأجسام، أو النظام الغذائي، أو التمرين الرياضي.

وتشير القرصنة الإلكترونية البيولوجية الأخلاقية بالإجمال إلى التقنيات التي تعدّل الأنظمة البيولوجية لدى البشر أو الكائنات الحيّة الأخرى. يتراوح ذلك من كمال الأجسام والمنشّطات العقلية–الدماغيّة، مروراً بتطوير علاجاتٍ لأمراض من خلال الاختبار الذاتي، ووصولاً إلى التلاعب بالجينات البشريّة من خلال تقنيّات التكرارات العنقودية المتناظرة القصيرة منتظمة التباعد كريسبر – بروتين كاس9 (CRISPR–Cas9 techniques) (صمويل [Samuel]، 2019؛ جريفِن [Griffin]، 2018).

أما السايبورغات، أي المتعضات السيبرناطيقية، فهُم أشخاص يستخدِمون الآلات لتعزيز الذكاء أو الحواس. ويتم الإقرار بنيل هاربيسون (Neil Harbisson)، وهو رجلٌ مصابٌ بعمى الألوان يستطيع أن "يسمع" الألوان من خلال هوائيٍ مزروعٍ في رأسه يعزف لحناً للألوان المختلفة أو أطوال موجات الضوء، على أنّه الشخص الأوّل المعترف به قانونياً من قِبَل حكومةٍ ما على أنّه سايبورغ، من خلال السماح له بأن يتم تضمين صورة جواز سفره في الجهاز المزروع في جسمه (دوناهو [Donahue]، 2017).

وبما أنّ إنترنت الأجسام هو مجالٌ واسع النطاق يتقاطع مع تعديل الجسم المُصمَّم للهواة، والمنتجات الاستهلاكية، والرعاية الطبية، يُعتبر فهْم منافعه ومخاطره أساسياً.

تكنولوجيات إنترنت الأجسام (IoB)

لقد تطوَّرَت تكنولوجيا إنترنت الأجسام (IoB) بسرعةٍ على امتداد مجموعةٍ من التطبيقات الطبيّة والاستهلاكيّة، حيث انضمَّت إلى الشركات الطبيّة القائمة والشركات التكنولوجية الكبيرة شركاتٌ ناشئةٌ أكثر حداثةً ومتخصصةٌ في مجال إنترنت الأجسام. إنّنا نقدّم في هذا القسْم أمثلةً حول أجهزة إنترنت الأجسام لتبيان مجموعة التكنولوجيات المتوفّرة أو قيد التطوير.

التطبيقات الطبيّة لإنترنت الأجسام (IoB)

لقد أدّت على مدار العقد الماضي التقدّمات في مجال التكنولوجيات الطبيّة وعلْم البيانات إلى نموٍّ كبيرٍ على مستوى الأجهزة الطبيّة المُمَكَّنَة من الإنترنت التي تَعِد بتوفير بيانات أفضل وأكثر دقّةً لدعْم رعاية المرضى وتحسين فعالية الرعاية الصحيّة. تُستَخْدَم هذه الأجهزة لمجموعةٍ من الأمراض والحالات، بما فيها داء السكري، والنوبات، ومرض باركنسون (الشلل الرعاش) (Parkinson's disease). يقدّم الجدول رقم 1 أمثلةً حول الأجهزة الطبية المُمَكَّنَة من الإنترنت والتي تُزرع في الجسم، في حين يبيّن الجدول رقم 2 بعض الأجهزة التي يمكن ارتداؤها (wearable devices) أو القائمة بذاتها (freestanding devices)؛[6] وإنّ جميع أجهزة إنترنت الأجسام هذه قيد الاستخدام أصلاً.

التطبيقات الاستهلاكيّة لإنترنت الأجسام (IoB)

لقد نَمَت السوق الاستهلاكيّة لإنترنت الأجسام (IoB) بسرعة، مع مجموعةٍ من الأجهزة الجديدة المتوفّرةِ أو قيد التطوير التي تهدف إلى تحسين الصحّة والراحة اليوميّتين وتوفير وسائل راحة أخرى. يحدّد الجدول رقم 3 بعض الأمثلة.

الاتّجاهات المستقبليّة: مزيدٌ من الاتصال، مزيدٌ من التكنولوجيات

ستمكّن التقدّمات في تكنولوجيا الإنترنت والاتصال عدداً أكبر من أجهزة إنترنت الأجسام (IoB) وإنترنت الأشياء (IoT) من الاتصال بعضها بالبعض الآخر وبسرعات أكبر بكثير. فبإمكان شبكة الجيل الخامس للاتصالات اللاسلكية الجوّالة (5G) أن تدعم مليون جهاز في مساحة قدم مربّع واحد، بالمقارنة مع شبكة الجيل الرابع (4G) التي باستطاعتها دعْم حوالي 4,000 جهاز في المساحة نفسها (زاينو [Zaino]، 2019). ويُتَوَقَّع أيضاً أن تُحسِّن شبكة تقنية الاتصال اللاسلكي 6 (الواي فاي 6) (Wi-Fi 6)، وهي الجيل التالي من تكنولوجيا تقنية الاتصال اللاسلكي (الواي فاي)،

الجدول رقم 1

أمثلة حول تكنولوجيات إنترنت الأجسام (IoB) الطبية المزروعة في الجسم

نوع إنترنت الأجسام (IoB)	الوصف
البنكرياس الاصطناعيّ (artifical pancreas)	يدمج نظام البنكرياس الاصطناعي (artificial pancreas) جهاز الرصد المستمرّ لمستوى الجلوكوز في الدمّ (continuous glucose monitor [CGM]) وتكنولوجيا مِضخَّة الإنسولين (insulin pump) مع خوارزميات الذكاء الاصطناعي (AI) التي تقوم بمكننة جرعات الإنسولين بالاعتماد على المُدخَلات من جهاز الرصد المستمرّ لمستوى الجلوكوز في الدمّ (بوتون [Boughton] وهوفوركا [Hovorka]، 2019). وقد سعى بعض مرضى داء السكريّ جاهدين إلى الحصول على مِضخّات الإنسولين القديمة من أجل قرصنة ثغرةٍ أمنيّة إلكترونياً، والتي تتيح وصْل المِضخّة بجهاز رصدٍ مستمرٍّ لمستوى الجلوكوز في الدمّ للحصول على بنكرياس اصطناعي مصمَّم للهواة (زهانغ [Zhang]، 2019).
واجهات الدماغ والحاسوب (brain–computer interfaces [BCIs])	تَسْتَخْدِم واجهات الدماغ والحاسوب (BCIs) الأقطاب الكهربائية التي تَصل الإشارات من الدماغ بحاسوبٍ ما. ويمكن أن تكون إمّا مزروعة في الدماغ أو غير باضِعة (أي يمكن ارتداؤها أو وضْعها على الجمجمة). تهدف واجهات الدماغ والحاسوب التي هي قيد التطوير إلى قراءة كلماتٍ كاملةٍ وطباعتها مباشرةً من الدماغ، أو إلى التحكُّم بالأطراف الاصطناعيّة انطلاقاً من العقل ("تخيُّل واجهة جديدة" ["Imagining a New Interface"]، 2019؛ إثرينغتون [Etherington]، 2019).
إشارات الدماغ الكهربائيّة لمرضى الباركنسون (الشلل الرعاش) (Parkinson)	إنّ تحفيز الدماغ العميق (deep brain stimulation)، وهو إجراء جراحيّ لزراعة الأقطاب الكهربائيّة في جزءٍ من الدماغ ووصْلها بجهازٍ كهربائيّ صغيرٍ مزروع في الصدر، كان الأوّل الذي جرت الموافقة على استخدامه لدى مرضى الباركنسون (الشّلل الرعاش) (Parkinson) في الولايات المتّحدة عام 2002 (لوموين وآخرون [LeMoyne et al.]، 2019). ففي السنوات الأخيرة، وبفضل التقدّمات الجديدة على غرار التحكُّم اللاسلكي من خلال هاتفٍ ذكيّ، أصبحَت التكنولوجيا أكثر دقّةً وذات طابع شخصيّ. تُمكّن الأسلاك الاتّجاهيّة (directional leads) طبيب كل مريض من توجيه العلاج إلى مناطق محددة من الدماغ (أكون [Okun]، 2019). ويتيح تطبيقٌ على هاتفٍ ذكيٍّ للمريض ضبْط الإعدادات من أجل تحسين النشاطات اليوميّة.
الأجهزة القوقعيّة (cochlear devices)	إنّ الجهاز القوقعيّ المزروع في الجسم (cochlear implant) هو جهاز إلكترونيّ يُعيد السمع جزئياً من خلال معالِج للأصوات (sound processor) يتمّ تركيبه خلْف الأذن من أجل التقاط الإشارات الصوتيّة. ينقل المعالِج تلك الإشارات إلى جهاز استقبال (receiver) مزروع تحت الجلد والذي يُحفّز بعدئذٍ العصب السمعيّ (سلاجِر وآخرون [Slager et al.]، 2019). وفي يونيو/حزيران 2017، تمّت الموافقة على الجهاز المزروع الأوّل والمقرون باتصّال لاسلكيّ مع الهواتف الذكيّة من قِبل إدارة الغذاء والدواء (FDA). يمكّن هذا الجهاز المرضى من رصْد السمع، وضبط الإعدادات، ورؤية المعلومات السمعيّة ذات الطابع الشخصيّ، وتحديد موقع معالِجات الأصوات الناقصة انطلاقاً من هواتفهم الذكيّة.
جهاز مزروع في الجسم لتنظيم ضربات القلب (implantable cardiac pacing)	يمكن أن توفّر منظِّمات ضربات القلب (cardiac pacemakers) الأجدّ، وأجهزة مقوم نُظُم القلب ومزيل رجفان بُطين القلب المزروعة في الجسم (implantable cardioverter defibrillators)، وأجهزة المساعَدة البُطَيْنِيّة (ventricular assist devices) معلوماتٍ آنيّةً ومستمرّة حول تقلّبات القلب لدى مريضٍ وتُمكّن إدارة الجهاز عن بُعْد من أجل مكننة عمليات الفحص التقنيّ، على غرار حالة البطاريّة، وإعاقة الأسلاك، وعتبات الاستشعار أو سرعة ضربات القلب (ستاشِل وآخرون [Stachel et al.]، 2013).
أجهزة رصْد مستوى الجلوكوز في الدمّ المزروعة في الجسم (implantable glucose monitors)	تقيس أجهزة الرصد المستمرّ لمستوى الجلوكوز في الدمّ (CGMs) مستويات الجلوكوز في الدمّ من خلال جهاز استشعار يوضَع تحت الجلد، وينقل جهاز الاستشعار القراءات عبر البلوتوث (Bluetooth) إلى أجهزة استقبال (receivers) محمولة يدوياً أو إلى تطبيقٍ على هاتفٍ ذكي. عندما تكون مستويات الجلوكوز مرتفعة جداً أو منخفضة جداً، يتلقّى المرضى إخطارات ليتمكّنوا من ضبْط مستوى الإنسولين لديهم أو تعزيز مستويات السكر في الدمّ (إدارة الغذاء والدواء [FDA]، 2018b).
دعامات القلب الذكية المزروعة في الجسم (implantable smart stents)	تُستخدم دعامات القلب (stents) تقليدياً من أجل إعادة فتْح الأوعية الدموية المسدودة (clogged blood vessels). وتُمكِّن الدعامات الذكيّة الرصد المستمرّ لتدفّق الدمّ عبْر الدعامة من أجل إنذار الجهات المزوِّدة باحتمال حدوث انسدادات جديدة (شِن وآخرون [Chen et al.]، 2018).
الحبوب الرقمية القابلة للهضم (ingestible digital pills)	وافَقَت إدارة الغذاء والدواء (FDA) عام 2017 على الحبّة الرقمية الأولى: إنّها أقراص أريبيبرازول (aripiprazole) مع جهاز استشعار قابل للهضم ومُضمَّن في الحبّة، يُسجِّل عملية أخْذ الدواء. يعمل النظام من خلال إرسال رسالةٍ من جهاز استشعار الحبّة إلى رقعةٍ يمكن ارتداؤها (wearable patch) والتي تنقل المعلومات إلى تطبيق على جهازٍ محمول، ليتمكّن المرضى من تتبُّع هضْم الدواء على هواتفهم الذكيّة. ويمكن للمرضى أن يسمحوا أيضاً لمقدّمي الرعاية لهم ولطبيبيهم بالوصول إلى المعلومات من خلال بوّابة على الإنترنت (تروث [Trauth] وبرونينغ [Browning]، 2018). وتتوفّر حالياً حبوب رقمية قابلة للهضم أخرى، بما فيها أدوية علاج الأورام عن طريق الفم (oral oncology drugs) مع جهاز استشعار رقميّ لتتبّع الالتزام، والجرعات، ومستويات نشاط المريض من أجل تطوير أنظمة جرعات أفضل للعلاجات الكيميائيّة.

الاتّصال من خلال السماح لمزيدٍ من الأجهزة بنقْل بيانات والتواصل مع الموجِّهات بشكلٍ متزامن (كاسترنايكس [Kastrenakes]، 2019). ويتم تطوير إنترنت الأقمار الاصطناعيّة (satellite internet) من أجل تعزيز توفُّر الإنترنت، بما في ذلك في المناطق النائية، من خلال وضْع آلاف الأقمار الاصطناعيّة في المدار الأرضيّ المنخفض (low Earth orbit) (غراش [Grush]، 2019؛ ستيدتِر [Staedter]، 2019). وستمكّن هذه التقدّمات تكنولوجيّات إنترنت الأشياء الاستهلاكيّة، مثل أنظمة المنازل الذكية، من الاتصال بأجهزة إنترنت الأجسام بحيث مثلاً، سيتمّ ربْط مُنَظِّم الحرارة (الترموستات) الذكيّ التابع لأحدهم بملابسه الذكيّة ليتمكّن من تنظيم درجة الحرارة تلقائياً في منزله. وسيزيد الاتصال الأكبر وحُزَم إنترنت الأجسام المنتشرة على نطاقٍ واسعٍ في الهواتف الذكيّة والأجهزة، والتي قد يجمع بعضها بيانات بدون علْم المُستَخْدِم، التتبّع الرقمي للمُستخدِمين على امتداد مجموعةٍ من السلوكيات.

يقترن بعض الأجهزة قيد التطوير، مثل العدسات اللاصقة للواقع المُعزَّز (augmented reality contact lens) أو الكتابة المباشرة في الدماغ (direct brain–writing)، بالقدرة على تغيير الحياة الاجتماعيّة بشكلٍ كبيرٍ من خلال تمكين تسجيل جميع تفاعلات شخصٍ ما وإعادة تشغيلها. إنّ الأجهزة العصبيّة لقراءة الدماغ وإرسال الإشارات (brain–reading and signaling

الجدول رقم 2
أمثلة حول تكنولوجيات إنترنت الأجسام (IoB) الطبية التي يمكن ارتداؤها والقائمة بذاتها

نوع إنترنت الأجسام (IoB)	الوصف
السجلّات الصحّيّة الإلكترونيّة (EHRs)	إنّها مستودعات للتاريخ الطبي لمريض ما (بما في ذلك تاريخ العلاج، والبيانات الجينيّة، وبيانات الأجهزة التي يمكن ارتداؤها، ومعلومات بيومتريّة أخرى) والتي توفّر معلومات آنية معنيّة بالمريض بشكلٍ فوريٍّ إلى المُستَخدِمين المصرّح لهم (دينه–لي وآخرون [Dinh–Le et al.]، 2019؛ مكتب المنسّق القومي لتكنولوجيا المعلومات الصحيّة [Office of the National Coordinator for Health Information Technology]، 2019).
مضخّات الحقن القائمة بذاتها (freestanding infusion pumps)	تُستخدم مضخّات الحقن القابلة للبرمجة (programmable infusion pumps) وأنظمة الحدّ من الجرعات الخاطئة (dose error–reduction systems) بشكلٍ شائعٍ حالياً في المستشفيات لإعطاء الدواء في الوريد. تَدْمُج هذه الأنظمة قواعد بيانات الأدوية مع مِضخّات الحقن وتتيح مكننة أنظمة الإنذار التي تنذرُ الجهات المزوّدة لدى حدوث أخطاء على مستوى البرمجة (جوليانو وآخرون [Giuliano et al.]، 2018). وتصل أنظمة أخرى مضخّة الحقن بسجلّ المريض الصحيّ الإلكتروني (EHR)، ما يقضي على الحاجة إلى برمجة المضخّة.
أسرّة المستشفيات المزوّدَة بأجهزة استشعار (sensor–equipped hospital beds)	إنّها أسرّة تضمّ أجهزة استشعار لدرجة حرارة الجسم، أو ضربات القلب، أو الدمّ، أو الأكسيجين، أو الضغط، أو بيانات أخرى يتم إرسالها إلى النظام المركزي في المستشفى وتُمَكِّن الجهات المزوّدة للخدمة الصحيّة من رصْد المؤشرات الحيوية لدى المرضى بشكلٍ آنيّ (بنتلاي [Bentley]، 2018).
مضخّات الإنسولين التي يمكن ارتداؤها (wearble insulin pumps)	إنّها أجهزة إلكترونيّة توفّر الإنسولين بشكلٍ مستمرّ في محاولةٍ لمحاكاة عملية إفراز البنكرياس للإنسولين الطبيعية. ويمكن دمج عملية إعطاء الإنسولين القابلة للبرمجة وزيادتها باستخدام أجهزة استشعار بيولوجيّة (biosensors) لجهاز الرصد المستمرّ لمستوى الجلوكوز في الدمّ (CGM) من أجل توفير تحكُّم آنيّ بمستويات السكّر في الدمّ ("كيف تعمل مضخّات الإنسولين" ["How Insulin Pumps Work"]، 2019).
أعضاء اصطناعيّة يمكن ارتداؤها (wearable prosthetics)	إنّها أعضاء اصطناعيّة مزوّدة بأجهزة استشعار إلكترونيّة للكشف عن حركات العضلات الدقيقة من أجل تشغيل الأطراف الاصطناعيّة (زلوتولو [Zlotolow] وكوزين [Kozin]، 2012). إنّ بعضها ممكَّنٌ من الإنترنت ويرسل تغذية راجِعة للمصنّعين من أجل تحسين التكنولوجيات؛ ويمكن أن يتتبّع بعضها المؤشرات الحيوية (يانغ وآخرون [Yang et al.]، 2017).
أجهزة رصْد النوبات التي يمكن ارتداؤها (wearble seizure monitors)	إنها كناية عن ساعات وغيرها من الأجهزة التي يمكن ارتداؤها والتي ترصد بشكلٍ مستمرٍّ المُستخدِم وتنذر أفراد العائلة ومقدّمي الرعاية لدى حصول أنماط حركة غير طبيعية مماثلة لتلك التي تتسبب بها النوبات، مثل تلك التي يتسبب بها الصرع (epilepsy) (ويكلوند [Wicklund]، 2018).

(neuro–devices) متوفّرة حالياً في السوق، وإنّما قد تنجح واجهات تكنولوجيا الدماغ المُحَسَّنَة (brain technology interfaces) في تحسين المعرفة، والذاكرة، والتحكُّم. ويمكن استخدام القراءة والكتابة في الدماغ في نهاية المطاف من أجل التأثير على أفكار الأشخاص لغايات خيّرةٍ أو خبيثة (المؤتمرات الدولية حول الحواسيب، والخصوصيّة وحماية البيانات [CPDP conferences]، 2018).

لقد أبدت الجيوش اهتماماً بتكنولوجيات إنترنت الأجسام من أجل تتبُّع صحّة العسكريين ورفاهيتهم، وتعزيز قدراتهم المعرفيّة والجسديّة، وتحسين التدريب، وتمكين قدرات القتال المُعزَّزَة، مثلاً باستخدام سماعات للواقع المعزّز (augmented–reality headsets) أو هياكل خارجية مزوَّدة بالتكنولوجيا (technology–infused exoskeletons) تتبَّع الخصائص الجسديّة لدى المحاربين كما أيضاً بشكلٍ محتمل حالتهم العقلية. وقد سعت الجيوش أيضاً إلى تطوير أجهزةٍ عصبيّة تُمكِّن التحكُّم بالأنظمة الجسديّة، مثل فكّ تشفير إشارات التحكُّم الحركيّ من الدماغ لتمكين طيّارٍ من تيسير طائرةٍ باستخدام أفكاره او أفكارها (إموندي [Emondi]، غير مؤرَّخ). وقد تُمَكِّن هذه القدرات اتّخاذ قرارات أسرع في ساحة المعركة وإنّما قد تُدخل أيضاً مخاطر جديدة بالنسبة إلى الحرب، مثل الهجمات الإلكترونيّة التي تؤثّر مباشرةً على دماغ جنديٍّ ما (بينيدجِك [Binnendjik]، مارلِر [Marler]، وبارتلِز [Bartels]، سيصدر قريباً).

قد تحفّز بيانات إنترنت الأجسام أيضاً التقدّمات الطبية، أو العسكريّة، أو الأخرى بطرقٍ غير مُتَوَقَّعَة. فعلى سبيل المثال، أُفيد في يونيو/حزيران 2019 بأنّ وزارة الدفاع الأمريكية (U.S. Department of Defense) تملك ليزر بالأشعة تحت الحمراء (infrared laser) يمكنه الكشف عن التوقيع القلبي الفريد (unique cardiac signature) لشخصٍ ما (قياس إيقاعات القلب الكهربائية) بدقّة تفوق نسبة 95 في المئة من مسافة 200 متر، حتّى من خلال بعض الملابس (دوفمان [Doffman]، 2019). في حال توفُّر قاعدة بيانات للسجلات الصحيّة الإلكترونيّة (EHRs) مع التواقيع القلبية، قد يكون من الممكن استخدام هذا الليزر لرصْد الأحداث القلبيّة لدى المريض في مستشفى أو لتحديد هويّة الأفراد المُحاربين في منطقة حرب عن بُعد وبدقّةٍ كبيرة (هامبلينج [Hambling]، 2019).

تقييم المنافع الصحيّة لإنترنت الأجسام

بحلول عام 2025، سيكون هناك أكثر من 41 مليار جهاز نشط لإنترنت الأشياء (IoT) (مؤسسة البيانات الدولية [International Data Corporation]، 2019)، تُولِّد 2.5 كوينتيليون بايت (quintillion bytes) من البيانات يومياً (مار [Marr]، 2018) حول البيئة، والنقل، والموقع الجغرافي، والنظام الغذائي، والتمرين الرياضي، والمسائل البيومترية، والتفاعلات الاجتماعية، وحياة البشر اليوميّة (فايولا [Faiola] وهولدِن [Holden]، 2017؛ بيوك وآخرون [Piwek et al.]، 2016). سيؤدي هذا الانفجار في أجهزة إنترنت الأشياء إلى ازدياد شعبية أجهزة إنترنت الأجسام (IoB). قد يوفّر إنترنت الأجسام منافع شخصية، مثل المتعة والراحة، ولكننا نركز هنا على تقييم ما إذا يمكن، مع زيادة فهْم

الجدول رقم 3
أمثلة حول تكنولوجيات إنترنت الأجسام (IoB) الاستهلاكيّة

نوع إنترنت الأجسام (IoB)	الوصف
أجهزة رصد الانتباه (attention monitors)	إنها نظارات تَسْتَخدِم نشاط الدماغ وحركات العينين لتتبُّع الانتباه. إنّها مُصمَّمَة ليتم استخدامها في المدارس أو أثناء القيادة وتوفّر تغذية راجعة صوتية أو لَمْسِيّة عندما تستشعر أنّ المستخدِم غير متنبّه (معهد ماساتشوسيتس لمختبر وسائل التكنولوجيا [Massachusetts Institute of Technology Media Lab]، 2019).
أجهزة الاستشعار المزروعة في الجسم (body–implanted sensors)	قد توفّر أجهزة الاستشعار البيولوجيّة المُدمجة في الأنسجة (tissue–integrated biosensors) قيد التطوير تتبُّعاً بيولوجياً أكثر دقّة وتوسّعاً بالمقارنة مع الأجهزة التقليدية التي يمكن ارتداؤها. قد يكون لأجهزة الاستشعار المزروعة هذه وظائف إضافيّة، على غرار واجهةٍ مُطعَّمَةٍ في الجلد (skin–grafted interface) تُمكّن المستَخدِم من التحكُّم بأجهزة أخرى عن بُعد (خان [Khan]، 2019). وقد تتبّع أجهزةِ استشعار التعرّف بالترددات اللاسلكيّة المُركَّبَة على الأسنان (tooth–mounted RFID sensors) والتي هي قيد التطوير المعلومات بشأن الجلوكوز، والملح، والكحول المُستَهلَكَة من قبَل المستَخدِم (سيلفر [Silver]، 2018).
الملابس المقرونة بأجهزة استشعار (clothing with sensors)	إنّها ملابس تحتوي على أجهزة استشعار لتسجيل درجة حرارة الجسم وتكييفها من أجل الحفاظ على راحة الشخص الذي يرتديها. ثمّة أيضاً منتجات للأطفال مثل الحفّاضات التي تَسْتَخْدِم تطبيقاً موصولاً بالبلوتوث (Bluetooth) للكشْف عن حركات الأمعاء والإبلاغ عنها (وترز [Waters]، 2019).
منتجات التكنولوجيا الأنثويّة (female technology products)	إنّ منتجات "التكنولوجيا الأنثوية" ("FemTech") هي تكنولوجيا مصمَّمَة لتحسين صحّة النساء. إنّها تشمل أجهزة يمكن ارتداؤها ومتصّلة بتطبيقات يمكنها قياس مخاط عنق الرحم (cervical mucus) لتتبّع الخصوبة، وأجهزة تساعد النساء على تقوية قاع الحوض (pelvic floor) لديهنّ من خلال التشجيع على ممارسة تمارين كيجِل (kegel exercises) وتتبُّعها، وأجهزة استشعار تقيس تقلّصات الولادة أثناء المخاض (جاراميلو [Jaramillo]، 2019).
أجهزة إنترنت الأجسام الاستهلاكيّة القائمة بذاتها (freestanding consumer IoB)	إنّها قطع أثاث وتجهيزات متّصلة بالإنترنت تتبّع رفاهية المستخدِم في المنزل وتقدّم التغذية الراجعة بشأنها. وهي تشمل المراحيض التي ترصد تدفّق البول ومستويات السكرّ وتفيد بالنتائج من خلال تطبيق (مار [Marr]، 2019a)؛ والمقاييس المُدمَجَة في التطبيقات الصحيّة لتتبُّع التقلّبات في وزن الجسم، ومؤشر كتلة الجسم (body–mass index)، ووزن الماء وتحليلها (روس [Ross]، 2019)؛ والأسِرَّة المُجَهَّزَة بأجهزة استشعار تتصل بتطبيقات لتتبُّع النوم من أجل جمْع بيانات حول أنماط النوم وتسجيلها (أبلباي [Appleby]، 2019).
الرقاقات الدقيقة المزروعة في الجسم (implantable microships)	إنّها الرقاقات الدقيقة للتعرّف بالترددات اللاسلكيّة (RFID) والاتصال القريب المدى (near–field communication [NFC]) المزروعة في أجسام البشر من أجل تخزين المعلومات، على غرار اسم شخص وعنوانه (مثل الرقاقات التي يضعها كثيرون من أصحاب الحيوانات في كلابهم). يمكن برمجة بعضها لفتح أقفال الأبواب أو للدفع مقابل السلع، بما يشبه أنظمة الدفع بالهواتف الذكية (جيلان [Gillan]، 2019).
أجهزة الاستشعار العقليّة والعاطفية (mental and emotional sensors)	تستطيع أجهزةِ الاستشعار القائمة بذاتها والتي يمكن ارتداؤها أن تقيّم الحالات العقلية والعاطفية لدى مستخدِمٍ ما، من خلال تحليل تعابير الوجه، ونبرات الصوت، وغيرها من الإشارات السمعية والبصريّة (داي [Day]، 2019؛ كليمو [Clymo]، 2018).
أجهزة مساعدَة الرؤية والسمع (vison and hearing aids)	إنها أجهزة مساعدَة الرؤية والسمع لتخزين التصوّر أو زيادته وتوفير إمكانيّة تسجيل الفيديو والصوت. وفي عام 2017، تم إصدار براءة الاختراع الأمريكية الأولى لعدسة مزروعة داخل العين (intraocular lens) مزوّدة بكاميرا لتسجيل الفيديو وقدرات لاسلكيّة (ستراثسبي كراون [Strathspey Crown]، 2017). ليست "السمّاعات" ("hearables") مُصمَّمة من أجل المساعدَة في حالة فقدان السمع فحسب وإنّما أيضاً للاتّصال بمساعدين فرضيين على الهواتف الذكية للكشْف عمّا إذا سقط المستخدِم وغيرها من المؤشرات السلوكية (تيبكِن [Tibken] وتشينج [Cheng]، 2018).
أجهزة تتبُّع الصحة التي يمكن ارتداؤها (wearable health trackers)	إنّها أساور، وساعات، وخواتم وتطبيقات على الهواتف الذكيّة تتبّع الخطوات، ومعدّلات ضربات القلب، وأنماط النوم، وغيرها من البيانات الجسديّة، على غرار كميّة الكحول التي استهلكها الشخص الذي يرتديها (تورك [Turk]، 2019). تعمل هذه الأجهزة من خلال استخدام أجهزة قياس التسارع (accelerometers) المتقدّمة وغيرها من أجهزة الاستشعار التي تستطيع أن تترجم الحركة إلى قياسات رقمية. وتوفّر أيضاً أجهزة متعددة تحليلات للبيانات والعروضات لتوفير معلومات مفصَّلَة بأشكالٍ يمكن الوصول إليها.
الأجهزة العصبية التي يمكن ارتداؤها (wearable neuro–devices)	تُسَجّل الأجهزة العصبيّة التي يمكن ارتداؤها على الرأس (Head–wearable neuro–devices) وترصد نشاط الدماغ وتحفّز الدماغ من خلال الإشارات الكهربائية. يُستَخدَم بعضها لتشجيع المستخدِم على تأدية تمارين للدماغ. وقد ترسل أخرى إشارات كهربائيّة إلى الدماغ من أجل معالجَة حالات مثل الألم المزمن، والاكتئاب، واضطراب نقص الانتباه (attention deficit disorder)، واضطراب ما بعْد الصدمة (الرّضح) (post–traumatic stress disorder) (كوتس ماك كول وآخرون [Coates McCall et al.]، 2019).

معلومات إنترنت الأجسام الخاصة بالمرضى، أن تحسّن الجهات المزوِّدة للخدمات الطبية علاج الصحة الوقائي، والكشف عن المرض في وقتٍ أبكر، وتحسين دقّة التشخيص، ومعالَجَة المرض بفعالية أكبر في نظام الرعاية الصحية الرسمي.

إنّنا في الأقسام التالية نوضّح أمثلةً حول إنترنت الأجسام الطبي والصحيّ والدليل بشأن منافعها. قد يمكّن إنترنت الأجسام وصولاً أوسع نطاقاً إلى الرعاية الصحيّة من خلال تمكين رعايةٍ صحيّةٍ غير مُكلِفَة "موزَّعة" أو "متوفَّرَة للجميع" أو من خلال الحدّ من الحاجة إلى التدخّل الطبيّ الخطير أو المُكْلِف. فمن خلال الوعي الصحي الأكبر، والوقاية المُحسَّنَة، والتدخُّل الأكثر فعاليّة، يقترن حتّى إنترنت الأجسام بإمكانيّة تخفيض تكاليف الرعاية الصحيّة. ولكن، من المهمّ الإشارة إلى أنّ العديد من تكنولوجيات إنترنت الأجسام هو جديد جداً ليكون قد طوَّرَ قاعدة أدلّة سريريّة حول النتائج الطويلة المدى. بدلاً من ذلك، يُفاد إلى حدٍّ كبيرٍ بأنّ المنافع المُحَقَّقَة حتّى تاريخه تحسِّن نواحي الفعالية اليوميّة بالنسبة إلى الجهات المُحَقَّقَة. وسيكون من الضروري تتبُّع قاعدة الأدلّة في الوقت الذي يسود فيه إنترنت الأجسام على نطاقٍ أوسع، وذلك من أجل فهْم الآثار الفعليّة لهذه الأجهزة على النتائج السريريّة.

الآثار على الطبّ الدقيق (Precision Medicine) والصحّة العامّة الدقيقة (Precision Public Health)

برز الطبّ الدقيق (precision medicine) والصحّة العامّة الدقيقة (precision public health) (دولي [Dolley]، 2018) ليطوّرا تدخّلات صحية تستهدف معالَجَة الحاجات الفريدة لمجموعات محدَّدَة. يتم تمكين الطبّ الدقيق من (1) مجموعة واسعة من الأبحاث الخاصّة بالمجموعة الفرعيّة والتي تشير إلى أنّ التدخّلات الصحيّة المختلفة ليست فعّالة على نطاقٍ واسع، وأنّ الاستراتيجيات الشرائحيّة قد تكون ضروريّة لتحسين العدالة؛ (2) زيادة البيانات الضخمة، والدقيقة، والمستمرّة، والطوليّة المولَّدَة من إنترنت الأجسام (IoB) والتي توفّر رؤية غير مسبوقة حول تجارب الأفراد؛ و(3) النضوج المتزامن لعلْم البيانات، والذي يتجاوز النطاقات الزمنيّة الضيّقة والآثار الأحادية المستوى لبطال التحاليل المصقولة، والمتعدّدة النطاقات الزمنيّة، والمتعددة المستويات، والمتقاطعة والتي تفسّر بشكلٍ أفضل التفاعلات المعقّدة بين المحدِّدات الاجتماعية، والسلوكيات، والصحّة. وتشير هذه العوامِل إلى أنّه، وإلى الحدّ الذي تُمَكّن فيه أجهزة إنترنت الأجسام الطب الدقيق، فهي قد تحسِّن النتائج الصحيّة بالنسبة إلى المجموعات الضعيفة أو تلك التي لم تحظَ بدراسةٍ كافية.

تجمع أجهزة إنترنت الأجسام البيانات الصحيّة المولَّدَة من الشخص (PGHD) حول جميع نواحي أنماط العيش والسلوكيات تقريباً، ما يشكِّل كنزاً ثميناً من المعلومات قد يطوّر بشكلٍ محتملٍ فهْم صحّة المجموعات على المدى الطويل والتدخّلات في مجال الصحّة العامّة الدقيقة. وتسمح البيانات الصحيّة المولَّدَة من الشخص التي تجمعها أجهزة إنترنت الأجسام الرصد المستمرّ للحالة الصحيّة في الوقت الآني، بالإضافة إلى جمْع بيانات طوليّة خارج نطاق الرصد المتقطّع الذي يجري في الوضعيّات السريريّة، وبالإضافة له (لاي وآخرون [Lai et al.]، 2017). وقد تنير البيانات الصحيّة المولَّدَة من الشخص الترابطات بين السلوكيات الفرديّة، والديموغرافيات الاجتماعية، والعوامل على مستوى المجموعات، لتكشف عن العلاقات المعقّدة بين الضواغِط الحادّة والمزمنة، والنظام الغذائي، وأنماط العيش، والصحة الإجمالية.

على الرغم من ذلك، إنّ البيانات الصحيّة المولَّدَة من الشخص قويّة بقدر التحاليل المُطوَّرَة لترجمة كميات كبيرة من البيانات غير المنظَّمَة والمتباينة إلى رؤى وتدخّلات صحيّة هادِفة. يُستخدم التعلُّم الآلي (machine learning)، والذكاء الاصطناعي (AI)، وغيرها من تقنيّات علْم البيانات بالإضافة إلى الإحصاءات التقليديّة من أجل التعرّف إلى الأنماط في مجموعات البيانات التجريبية الكبيرة، وإصدار التنبّؤات بالاستناد إليها (لوبتون [Lupton]، 2013؛ لوبتون [Lupton]، 2014). وقد تمّ دمْج الذكاء الاصطناعي بنجاحٍ في دعْم القرارات في الاختصاصات الكثيفة البيانات مثل التصوير بالأشعّة، وعلْم الأمراض (الباثولوجيا)، وطبّ العيون (يو [Yu] وكوهان [Kohane]، 2019). وعلى عكْس التصاميم المدفوعة من الفرضيات، يتيح علْم البيانات الترابطات الشبكيّة والمتعدّدة المستويات بين متغيّرات متعدّدة متعلّقة بالنتائج الصحيّة لتطوير توقّعات للمخاطر المُعَقَّدة للمساعدَة في عملية صنْع القرارات. إنّه يمكّن تحديد المؤشّرات الرقميّة للصحّة التي يمكن استخدامها لرصْد السلوكيات السليمة، والتأثير عليها، والحفاظ عليها في الوقت الآني. فعلى سبيل المثال، تُبَيِّن الدراسات الأخيرة أنّ التغييرات الفرديّة في تواتر النشاط الجسديّ وكثافته قد تُنْبئ بالاكتئاب (كومار وآخرون [Kumar et al.]، 2018)، وأنّ البيانات السمعيّة التي يتمّ جمْعها من محادثات الأشخاص عبْر الهواتف الجوّالة قد تُنْبئ بضعْفٍ إدراكيّ (cognitive impairment) (ستاك وآخرون [Stück et al.]، 2018). تسلّط هذه الدراسات الضوء على فرصةٍ كبيرةٍ لاستخدام إنترنت الأجسام لتشكيل حلقة من التغذيات الراجعة التآزرية بين الباحثين، والمهنيين في المجال الصحي، والمستهلِكين.

لا تزال الأقليات العرقية والإثنيّة، والأشخاص المحرومون اجتماعياً واقتصادياً، والمجموعات التي تتعرّض للتمييز تختبر نتائج صحيّة سلبيّة وغير متناسبة (المركز الوطني للإحصاءات الصحيّة [National Center for Health Statistics]، 2016)، على الرغم من عقودٍ من الأبحاث التي تربط المحدِّدات الاجتماعيّة الفرديّة للصحّة، مثل الديموغرافيات (مثلاً، السنّ، والجنس، والعرق) أو الخصائص الاجتماعيّة أو خصائص المجموعة (مثلاً، العمل، والحي، والسكن)، والسلوكيات المرتبطة بها (مثل، النظام الغذائي، والتمارين الرياضية، والمخدرات، والكحول) بالاختلافات على مستوى النتائج الصحيّة (مارموت [Marmot]، 2005). ولا تزال مقاربات متعدّدة في مجال الصحّة العامّة تستخدِم متوسّطات المجموعة لتشكيل تدخّلات على شكل "مقاس واحد يلائم الجميع" من أجل زيادة احتمال تحقيق النتائج الفضلى لأغلبية الأشخاص (غلاسغو [Glasgow]، كوان [Kwan]، وماتلوك [Matlock]، 2018؛ برايفمَن وآخرون [Braveman et al.]، 2005)، الأمر الذي قد يساهم في النتائج السلبية غير المتناسبة. وقد يساعد إنترنت الأجسام في مكافحة هذا الأمر من خلال تمكين الطب الدقيق والصحة العامة الدقيقة بشكلٍ إضافيّ.

الآثار على الرعاية الطبيّة

السجلات الصحيّة الإلكترونية (Electronic Health Records)

يتمّ الترويج للسجلات الصحيّة الإلكترونية (EHRs) من قِبَل مكتب المنسّق القومي لتكنولوجيا المعلومات الصحيّة (Office of the National Coordinator for Health Information Technology)، وهو جزء من وزارة الصحة والخدمات البشرية الأمريكية (U.S Department of Health and Human Services)، من أجل تحسين قابلية التشغيل المتبادل للبيانات

الصحيّة. إنّ السجلات الصحيّة الإلكترونيّة هي مستودعات رقميّة للتاريخ الطبي لمريضٍ ما، توفّر معلومات آنيّة معنيّة بالمريض بشكلٍ فوريّ إلى المُستَخدِمين المصرَّح لهم. وعلى الرغم من أنّ السجلّات الصحيّة الإلكترونيّة تضمّ التواريخ الطبيّة وتواريخ العلاجات الخاصة بالمرضى، إنّها مصمَّمَة لتتجاوز البيانات السريرية القياسيّة التي يتمّ جمْعها في مكتب جهةٍ مزوِّدةٍ ويمكن أن تشمل السلوكيات، والأوضاع المعيشيّة، والتاريخ العائلي. وقد تضمّ أيضاً السجلات الصحيّة الإلكترونيّة المتطوّرة بيانات جينيّة وبيانات من أجهزة يمكن ارتداؤها ومن مجموعة من المصادر الأخرى.

تيسّر السجلات الصحيّة الإلكترونية الممارسة المرتكزة إلى الأدلة من خلال دمْج المبادئ التوجيهية السريريّة وأدوات المكننة التي توفّر للجهات المزوّدة توصيات مُحدَّثَة متعلّقة برعاية المرضى (آلِن–غراهام وآخرون [Allen–Graham et al.]، 2018). فهي قد برْهَنَت عن إنتاجيّةٍ وإدارة موارد مُحسَّنَتين بالنسبة إلى المستشفيات وعن جودة مُحسَّنَة لرعاية المرضى (إنتزِريدو [Entzeridou]، ماركوبولو [Markopoulou]، وموﻻكي [Mollaki]، 2018). على سبيل المثال، أفادت نسبة 88 في المئة من المعنيين بالممارسات في دراسة استقصائية وطنيّة حديثة أنّ سجلّهم الصحيّ الإلكتروني ينتج منافع سريريّة بالنسبة إلى المرضى، وأفادت نسبة 75 في المئة أنّ السجلات الصحيّة الإلكترونيّة تتيح تقديم رعاية أفضل. وقد شمَلَت أسباب المنافع السريريّة الحدّ من الأخطاء المتعلّقة بالأدوية، وتحسين سلامة المرضى، وتحسين الإدارة المخصَّصَة (جامون وآخرون [Jamoon et al.]، 2012).

ومع العلم أنّ إنترنت الأجسام يضخّ بيانات أكثر غنى وأكثر تبايناً في السجلات الصحيّة الإلكترونية، ثمّة سبب لتوقُّع أنه سيساعد الباحثين والأخصائيين السريريين في فهْم الارتباطات بين البيئة، والسلوكيات، والصحة، والمرض.

التطبيقات داخل المستشفيات

قد يتيح إنترنت الأجسام (IoB) تحسين إدارة الرعاية وإعطاء الأدوية في الوضعيات داخل المستشفيات. فقد تحدّ الآلات المتصّلة فيما بينها والتي تتبادل البيانات (مثل السجلات الصحية الإلكترونية [EHRs]، ودعْم القرارات السريريّة، وإعطاء الأدوية، وأجهزة التنفّس الاصطناعيّ، ومِضَخّات الحقن، وأسِرَّة المستشفيات) من الأخطاء وتتيح لفريق عمل المستشفى قضاء وقت أقلّ للبحث عن سجلّات المرضى أو المعلومات حول الأدوية، وتتبّع اللوائح، وإجراء جردات اللوازم.

فعلى سبيل المثال، تُستخدم مِضخّات الحقن القابلة للبرمجة (programmable infusion pumps) وأنظمة الحدّ من الجرعات الخاطئة (dose error–reduction systems) بشكلٍ شائعٍ حالياً في المستشفيات لإعطاء الدواء في الوريد، بطريقةٍ دقيقةٍ ومراقَبَة. على الرغم من ذلك، قد تحدث الأخطاء المتعلقة بالأدوية نتيجةً لخطأ يقترفه المُستَخدِم في برمجة المِضخّة. تتيح مِضخّات الحقن الأجدّ المكننة الخوارزميّة لأنظمة الإنذار التي تنذر الجهات المزوِّدة لدى حدوث أخطاء برمجة من خلال مطابقة الأدوية مع

قد يتيح إنترنت الأجسام تحسين (IoB) إدارة الرعاية وإعطاء الأدوية في الوضعيات داخل المستشفيات.

المبادئ التوجيهية بشأن الجرعات (جوليانو وآخرون [Giuliano et al.]، 2018). ويدفع الدمْج بين الممارسات السريريّة وفي الوريد (intravenous clinical integration) (دوني وآخرون [Downey et al.]، 2018) بهذا الأمر خطوةً إلى الأمام، حيث يُدخِل طبيبٌ ما أمر الدواء في السجل الصحي الإلكتروني (EHR)، ويتم نقْل هذا الأمر مباشرةً إلى مِضخّة الحقن مع معدّلات التدفق والجرعات الصحيحة.

وتستفيد أسِرَّة المستشفيات المزوَّدة بأجهزة استشعار (sensor–equipped hospital beds) من الفترات الزمنية الطويلة التي يقضيها المرضى في السرير لتتبُّع مؤشراتهم الحيويّة وتحميل البيانات في سجلّهم الصحيّ الإلكتروني. يمكن أن تقيس أجهزة الاستشعار درجة حرارة الجسم، ومعدل ضربات القلب، والدمّ، والأكسيجين، والضغط، ودخول السوائل إلى الجسم وخروجها منه، وغيرها من المؤشرات. ويمكن للجهات المزوِّدة أن تُراجع حالة مرضاها وترصدها عن بُعد وأن تتلقّى رسائل إنذار في حال حدوث أي تغيير مفاجئ في حالة المريض (دوني وآخرون [Downey et al.]، 2018). وقد كَشَفَت مراجعة منهجيّة أن الرصْد المستمرّ عن طريق القياس عن بُعد (continuous telemetry monitoring) في المستشفيات من خلال الأسِرَّة المجهَّزَة بأجهزة استشعار والأنظمة الأخرى قد حسَّنَ نتائج المرضى وحدَّ من الوقت الذي يتم قضاؤه في الرعاية الحرجة للمرضى على عكْس الرصد المتقطّع (دوني وآخرون [Downey et al.]، 2018)، ما يشير إلى أنّ تطبيق الرصد غير الباضِع على نطاقٍ واسعٍ قد يُحسِّن رعاية المرضى.

العلاج في العيادات الخارجيّة وإدارة الالتزام

لقد اتَّضَح أنّ رصد العلاج عن طريق إنترنت الأجسام (IoB) يساعد المرضى على الالتزام بجداول علاجهم الزمنيّة مع السماح للأطباء في الوقت عينه بتتبّع الامتثال للوصفات الطبيّة. فقد وافَقَت إدارة الغذاء والدواء (FDA) عام 2017 على الحبّة الرقمية (digital pill) الأولى: إنّها أقراص أريبيبرازول (aripiprazole) مع جهاز استشعار قابل للهضم ومُضمَّن في الحبّة، يُسجِّل عملية أخْذ الدواء. إنّ المنتَج موافقٌ عليه لعلاج مرض انفصام الشخصيّة (schizophrenia)، والعلاج الحادّ لنوبات الهوس والنوبات

المختلطة المرتبطة باضطراب المزاج الثنائي القطب من النوع الأوّل (bipolar I disorder)، ولاستخدامها بمثابة علاج إضافيّ للاكتئاب لدى الراشدين. ويعتبَر الالتزام بالعلاج أساسياً بالنسبة إلى هذه الاضطرابات وهو يشكّل العامِل الأكبر والوحيد الذي يُنْبئ بانتكاس المرضى (بابولا [Papola]، جَسْتَلدون [Gastaldon]، وأستوزي [Ostuzzi]، 2018). يعمل النظام من خلال إرسال رسالةٍ من جهاز استشعار الحبّة إلى رقعةٍ يمكن ارتداؤها (wearable patch). وتنقل الرقعة المعلومات إلى تطبيق على جهازٍ محمول، ليتمكّن المرضى من تتبُّع هضْم الدواء على هواتفهم الذكيّة. ويمكن للمرضى أن يسمحوا أيضاً لمقدّمي الرعاية لهم ولطبيبهم بالوصول إلى المعلومات من خلال بوّابة على الإنترنت (تروث [Trauth] وبرونينج [Browning]، 2018).

انطلاقاً من النجاح الذي حققته تلك الحبّة الرقميّة، تم أيضاً تطوير دواء عن طريق الفمّ لعلاج الأورام مقرون بجهاز استشعار رقميّ لتتبُّع الالتزام، والجرعات، ومستويات نشاط المريض من أجل تحسين أنظمة الجرعات للعلاجات الكيميائيّة. وفي نهاية المطاف، قد تمنح علاجات مماثلة مُمَكَّنَة من إنترنت الأجسام الجهات المزوِّدة ومقدّمي الرعاية رؤى جديدة، وتتيح رعاية المرضى عن بُعد، وتحول دون دخول المستشفى، وتحسِّن الاستجابة للعلاج (بلومان [Plowman]، بيترز–ستريكلاند [Peters–Strickland]، وسافاج [Savage]، 2018).

رصْد الحالات المزمنة عن بُعد

لقد أدّت الظاهرة العالمية لشيخوخة السكّان (الأمم المتّحدة [United Nations]، 2015؛ هاربر [Harper]، 2006) إلى ارتفاعٍ كبيرٍ في حدوث الأمراض غير السارية (noncommunicable diseases [NCDs]) المزمنة وانتشارها. يموت كل عام حوالي 41 مليون شخص نتيجةً للأمراض غير السارية، ما يُمثّل نسبة 71 في المئة من إجمالي الوفيات العالمية. وتستحوذ الأمراض غير السارية على مبلغٍ غير متناسبٍ من الإنفاق على الرعاية الصحية، إذْ تستحوذ نسبة الخمسة في المئة تقريباً الأكثر كلفةً من المرضى على حوالي 50 في المئة من تكاليف الرعاية الصحية (منظّمة الصحة العالمية [World Health Organization]، 2018).

يُعدّ إنترنت الأجسام (IoB) مقاربةً واعدةً لتطوير أنظمة رصْد الصحّة الآني عن بُعد للمرضى المصابين بأمراض غير سارية، ومعظمهم من مرضى داء السكري والقلب. إنّ داء السكري متفشٍّ في أغلبية المناطق في العالَم. وتَعِد التطورات الأخيرة في تكنولوجيا البنكرياس الاصطناعي، المُمكَّنَة من مجموعة من أجهزة إنترنت الأجسام، بتحكُّمٍ أفضل بمستوى السكّر في الدم وبرصْدٍ أفضل للمرضى عن بُعد (جارج وآخرون [Garg et al.]، 2017).

فقد برهن البحث أنّ رصْد المؤشرات الحيويّة قد يساعد على الحدّ من دخول المستشفى من جديد من خلال الكشْف المبكر عن الانحرافات عن الحالة الطبيعية وإتاحة التدخّلات الملائمة وفي الوقت المناسب (فانوتشي وآخرون [Fanucci et al.]، 2013). وقد وافَقَت إدارة الغذاء والدواء (FDA) على ساعة يد تتبِّع الرجفان الأُذَيْني (atrial fibrillation)، فتُنذِر المرضى من أنّهم قد يحتاجون إلى مراجعة طبيب (آبل [Apple]، 2018). بالإضافة إلى ذلك، وَجَدَت دراسةٌ أجراها مركز السياسات الصحية المتصلة (Center of Connected Health Policy) أنّ رصْد المرضى الذين يعانون من فَشَل القلب عن بُعد باستخدام أجهزة إنترنت الأجسام أدّى إلى خفْض معدّل القبول في المستشفيات من جديد بعْد مرور 30 يوماً بمعدّل 50 في المئة (أجبولا وآخرون [Agboola et al.]، 2015). وقد تمّ افتراض أنّ الكشف المبكر والتدخّل من خلال الرصد عن بُعد كانا الدافعيْن الأوليَيْن للحد من هذا المعدّل.

إنقاذ الحياة من خلال الإنذارات

يمكن أن تجمع أجهزة إنترنت الأجسام (IoB) بيانات حيويّة لإرسال إنذارات طبية إلى الأطباء، والمرضى، ومقدّمي الرعاية. فقد وافَقَت إدارة الغذاء والدواء (FDA) على ساعة يد لرصْد النوبات تكشف عن أنماط الحركة غير الطبيعية. فعندما تكشف هذه الساعة عن خاصيّة حركة الاهتزاز المتكرّرة المتعلقة ببعض النوبات، ترسل فوراً إنذارات على شكل رسالة نصيّة واتصال هاتفي إلى الجهات المتلقيّة للإنذار التي يحددها المريض. وقد كَشَفَت الدراسات السريريّة أن الساعة كانت قادرة على تحديد النوبات بشكلٍ صحيح لدى المرضى الراشدين والمرضى الأطفال على حد سواء بمعدّل صفر تقريباً من النتائج الإيجابية الخاطئة (جوتيريز وآخرون [Gutierrez et al.]، 2018).

قد يتضح أيضاً أنّ أجهزة إنترنت الأجسام مفيدةً في إرشاد العلاج بالنسبة إلى الأشخاص العاجزين عن الكلام أو التعبير عن أعراضهم أو أفكارهم، مثل الأطفال، أو ضحايا الجلطات، أو مرضى الخَرَف، وذلك من خلال إنذار مقدّمي الرعاية بشأن التغيرات البارزة في المؤشرات الحيوية، على سبيل المثال. وقد يستفيد المواطنون الكبار في السنّ أيضاً مثلاً من أجهزة الاستشعار التي تستطيع الكشف عن حالات السقوط لاستدعاء خدمات الطوارئ. ووَجَد الباحثون الذين يستخدمون تكنولوجيا أجهزة الاستشعار هذه أنّه كان من الممكن حتّى التنبؤ بحصول حادثة سقوط بالاعتماد على أنماط مشي المستَخدِم (سكوت [Scott]، 2018).

مراقبة المرض

تعتمد مراقبة الأمراض على جمْع البيانات من عددٍ كبيرٍ من الأفراد والمستشفيات الممتدّة على مسافاتٍ جغرافيّةٍ كبيرة. ويُعتَبَر إنترنت الأجسام (IoB) ملائماً جدّاً بوجهٍ خاص لهذا الغرض (ستيل [Steele] وكلارك [Clarke]، 2013) لأنّ أجهزة الاستشعار المُضمَّنَة في الهواتف الذكيّة، والأجهزة التي يمكن ارتداؤها، والمنشآت العامّة مثل المراحيض أو مقابض الأبواب قد تُستَخدَم جميعها للكشف عن وجود المرض ولتتبُّع انتشاره بين السكّان. قد يُمكِّن هذا

الأمر التدخّل في حالات بعض الأوبئة أو الجائحات مثل الحصبة (measles)، أو الإيبولا (Ebola)، أو الإنفلونزا (flu). والجدير بالذكر بوجهٍ خاص هو قدرة أجهزة إنترنت الأجسام على تحديد عدد الأشخاص الذين تعرّضوا لمرضٍ ما بدون أن تظهر عليهم أي عوارض، أي الذين تُطلَق عليهم تسمية حاملو العدوى الصامتون (silent carriers) والذين يُعتبرون أساسيين لفهْم معدّلات حدوث المرض. وقد يكون إنترنت الأجسام حلاً فعّالاً لتحدّي العدد الكلّي الأساسي هذا (بورسيل وآخرون [Purcell et al.]، 2016) من خلال تمكين تتبُّع سلوك حاملي العدوى الصامتين وتحليله.

حالات عدم اليقين المتعلّقة بمنافع إنترنت الأجسام (IoB): كيف تتراكَم الوعود

في حين تَحَقَّقَت منافع متعدّدة لإنترنت الأجسام (IoB) في القطاع الطبي الرسمي، لا تزال حالات عدم اليقين قائمة. فقد تحول الوقائع العمليّة دون الوفاء بعديدٍ من وعود إنترنت الأجسام، أقلّه على المدى القصير؛ فعلى سبيل المثال، كانت قابليّة التشغيل المتبادل الوظيفي للسجلات الصحية الإلكترونية (EHRs) تحدّياً (سوليفان [Sullivan]، 2018)، كما يبقى الانتقال عملاً قيد التقدّم. كان للجهات المزوِّدة للخدمات الطبيّة ردة فعل مختلطة إزاء مقاربات المرضى الأخرى للمساعدة الذاتية، على غرار البحث عن المعلومات عبْر المجتمعات الصحيّة على شبكة الإنترنت (روبيرت وآخرون [Rupert et al.]، 2014). وكما هي الحال بالنسبة إلى الظواهر الأخرى المُصمّمة للهواة (DIY) (مثلاً، التحوُّل إلى أجهزة صرْف الأموال الآلي)، قد تَحْدُث تغييرات طويلة المدى على مستوى النشاط الاقتصادي (مثل التحوُّلات في أنماط الاستهلاك الممكَّنَة من الإنفاق المرتجل). قد تكون هذه التغييرات سابقة لأوانها لتُفهَم الآن وإنما يجب رصْدها من قِبَل الباحثين مع تطوُّر إنترنت الأجسام والرقمنة الأخرى.

تقييم مخاطر إنترنت الأجسام

إنّ برمجيات الحاسوب ضعيفة بطبيعتها في وجه العيوب غير المقصودة أو الإساءة الخبيثة. فيمكن استخدام نقاط الضعف في الرمز لسرقة المعلومات التي جَمَعَها الجهاز أو للتلاعب بها، أو لتعطيل تشغيله، أو للتسبب بخلاف ذلك بعَمَلِه بطرقٍ غير متوقّعةٍ أو غير مقصودة. تعاني تكنولوجيات إنترنت الأجسام (IoB) من ناقلات الهجمات نفسها كما أجهزة إنترنت الأشياء (IoT) والمعدات الحاسوبية الأخرى، إلّا أنّ أجهزة إنترنت الأجسام تقترن بمخاطر مُعزَّزَة ناتِجةَ عن التقاء خصائص متعددة، بما فيها الاتصال بالجسم، ونوع المعلومات المجموعة ومداها، وكيفية استخدام المعلومات. يولّف الجدول رقم 4 مخاطر إنترنت الأجسام بمثابة دالّة لأولئك الذين قد يحصلون على وصولٍ غير مصرَّح به، أو غير قانوني، أو غير متوقَّع إلى البيانات أو، من خلال الجهاز، إلى الجسم؛ ونقاط الضعف المتوقَّعَة؛ والعواقِب المحتملَة. وإنّ أجهزة إنترنت الأجسام التي يُرَجَّح أن تؤدي إلى العواقِب الأكثر خطورة (العمود الأيسر من الجدول رقم 4) هي تلك التي تقترن بعددٍ كبير من نقاط الضعف (العمود الأوسط من الجدول رقم 4) والتي تستغلّها جهات فاعلة متعدّدة (العمود الأيمن من الجدول رقم 4).

المخاطر من حيث الأمن العالمي، والقومي والشخصي

أصدَرَت شركة اللياقة البدنيّة سترافا (Strava) عام 2018 معلوماتٍ مفصّلَةَ حول الموقع الجغرافي لطرقات التمارين الرياضية لمستَخدِميها. وكانت وزارة الدفاع الأمريكيّة (Department of Defense) تشجّع أجهزة تتبُّع الصحّة في محاولةٍ لمكافحة تفشي وباء السمنة (obesity epidemic) وقد أجرَت برنامجاً إرشادياً قدّم أجهزة لتتبُّع اللياقة البدنية لأكثر من 2,000 جندي عام 2013 (بوشاتز [Bushatz]، 2013) و20,000 جندي عام 2015

الجدول رقم 4

مخاطر إنترنت الأجسام (IoB): الوصول غير المتوقَّع، ونقاط الضعف، والنتائج

مَن قد يكتسب الوصول؟	ما هي نقاط الضعف المحتملة؟	ما هي العواقِب المُمْكِنَة؟
• المجرمون • القراصنة الإلكترونيون (مثلاً، الباحثون في مجال الأمن، والهواة، والمهاجمون الخبيثون) • وسطاء البيانات • مراكز دمْج البيانات • أرباب العمل • المدارس • الجهات المزوِّدة للرعاية الصحيّة • شركات التأمين • المصنّعون • نظام العدالة الجنائيّة • الحكومات	• الاعتماد الجسدي على الجهاز لأغراض صحيّة أو وظيفيّة • جمْع البيانات الحساسة، أو حيازتها، أو تعميمها • الاتصال بالإنترنت • الفجوات التنظيمية • المعدات الحاسوبيّة • البرمجيات	• الموت أو الضرر الجسدي الناتج عن العطل أو القرصنة الإلكترونية • تحديات الأمن العالمي والقومي • اختراق البيانات • جمْع البيانات أو تبادلها السلبيان بدون الموافقة المستنيرة • سوء استخدام البيانات أو استخداماتها غير المتوقَّعة • تحديد الهوية الشخصية • زيادة التباينات الصحيّة • الإرغام على قبول الأجهزة • انتهاك استقلالية الجسم

(ليلي [Lilley]، 2015). وكانت الخرائط التي أصدرَتْها شركة سترافا مفصّلةً وشاملةً جداً لدرجة أنّها كَشَفَت بشكلٍ مُحتَمَلٍ في نهاية المطاف قواعِد عسكرية ومعسكرات مخفية لأفراد عسكريين ومدنيين أمريكيين وأنماط عيش العسكريين (هيرن [Hern]، 2018). وبعد الحادثة، عدَّل الجيش سياساته ولم يَعُد يسمح للعسكريين المنتشرين باستخدام هذه التطبيقات أو الأجهزة (كوب [Copp]، 2018).

ليس هذا سوى مثل واحد حول كيف يمكن أن يشكِّل انفجار الابتكار واعتماد أجهزة إنترنت الأجسام (IoB) مخاطر من حيث الأمن العالمي والقومي. يمكن توقُّع بعض هذه المخاطر. فعلى سبيل المثال، نَظَرَ الأطباء في إمكانيّة استخدام مُنظِّم ضربات القلب المزروع في جسم نائب الرئيس ديك شيني (Vice President Dick Cheney) لاغتياله. لقد كان مُنظِّم ضربات القلب الأصلي المزروع في جسم شيني مجهَّزاً بميزةٍ للرصد اللاسلكي، والتي كان من المحتمل قرصنتها إلكترونياً. وفي عام 2007، تمّ استبدال جهاز شيني بجهازٍ آخر بدون قدرةٍ لاسلكيّة (فاس [Vaas]، 2013). فقد لا يمكن توقُّع مخاطر أخرى لإنترنت الاجسام أو معالجتها بالسهولة نفسها.

إنّ اتصال الأجهزة المتصلة بالإنترنت قيد التقدّم من حيث النوع والجودة وسيكون مَمَكَّناً بشكلٍ إضافيٍّ من تكنولوجيات الاتصالات، مثل الجيل الخامس (5G)، وهو الجيل التالي من الاتصالات اللاسلكية الجوّالة (الواي–فاي) (Wi–Fi)، وإنترنت الأقمار الاصطناعية. ولكن من المرجَّح أن يتم استهداف أنظمة الاتصالات من قِبَل الدول الخصم والقراصنة الإلكترونيين المجرمين. وقد اتَّضَح أصلاً أنّ بروتوكولات تقنية الاتصال اللاسلكي (الواي فاي) الجديدة تقترن بعيوبٍ أمنيّة (جودِن [Goodin]، 2009)؛[7] فقد بَرَزَت مخاوف بشأن الجيل الخامس (الجيل القادم [Ng]، 2019)، لاسيّما بالنظر إلى هيمنة البائعين الصينيين في مجال إمداد المعدّات الحاسوبيّة والخدمات عالمياً (براين–لو وآخرون [Bryan–Low et al.]، 2019)؛ وقد تهدّد البرامج الفضائية المضادة (counterspace programs) المتنامية في الصين وروسيا الأنظمة المرتكزة إلى الأقمار الاصطناعيّة الأمريكية (وكالة استخبارات الدفاع [Defense Intelligence Agency]، 2019). كما قد يوفّر ازدياد الاتصال في أجهزة إنترنت الأشياء (IoT) وإنترنت الأجسام مساحة هجوم متزايدة تُدخِل مزيداً من نقاط الضعف من خلال هذه الشبكات.[8]

لطالما شكّل الاستثمار الأجنبيّ في الشركات الأمريكيّة وشراؤها مصدر قلقٍ بسبب المخاطر من حيث الأمن القومي. فقد تأسَّسَت لجنة الاستثمار الأجنبي في الولايات المتحدة (Committee on Foreign Investment in the United States [CFIUS]) عام 1975 لتحليل المعاملات التي قد تكون لها تداعيات على المصالح القوميّة الأمريكية (جاكسون [Jackson]، 2019). قد توصي لجنة الاستثمار الأجنبي في الولايات المتحدة بتعليق الاستثمار في شركةٍ أمريكية أو بحظْره إذا كان هذا الاستثمار ليسمح لكيانٍ أجنبيّ بالاحتفاظ ببيانات شخصيّة حساسّة تخصّ المواطنين الأمريكيين أو جمْعها. وبالتالي، ستدعو الحاجة إلى دراسة الاستثمار الخارجي في شركات إنترنت الأجسام عن كثب. وفي عام 2016، استحوذَت الشركة الصينيّة كونلون (Kunlun) على جريندر (Grindr)، وهو تطبيق مشهور لمواعدة المثليين الجنسيين، وإنّما وافَقَت على بيعه في مايو/أيار 2019 بعْد تحقيقٍ أجرته لجنة الاستثمار الأجنبي في الولايات المتحدة (وانج [Wang]، 2019). وفي حين لم تكشف لجنة الاستثمار الأجنبي في الولايات المتحدة عن الأسباب المحددة لاعتراضها على الملكية الصينية لقواعد بيانات جريندِر، تثير المعلومات حول موقع المُستَخدِمين، ورسائلهم، وحالتهم من حيث فيروس نقْص المناعة (HIV) مخاوف متعلّقة بابتزاز المسؤولين أو المقاولين الحكوميين الأمريكيين (بويرل دانزمان [Bauerle Danzman] وغيرتز [Gertz]، 2019).

وتماماً كما يمكن استخدام الحيازة الأجنبية لبيانات حول عادات الأمريكيين من حيث المواعدة أو حالة فيروس نقص المناعة لأغراض شريرة، يمكن استغلال بينات المستهلِكين الأمريكيين البيومترية والصحيّة من قِبَل الخصوم الذين يجمعون البينات من مصادر مختلفة لبناء ملفات شخصيّة مفصّلة لأهدافهم الأمريكية. ففي مايو/أيار 2019، تمّ اتّهام جهات فاعِلَة صينية بانتحال شخصيّة، وقرصنة حواسيب إلكترونياً، والتآمر لارتكاب الاحتيال في عملية القرصنة الإلكترونيّة عام 2015 لشركة أنثيم (Anthem)، وهي إحدى أكبر شركات التأمين الصحي في الولايات المتحدة (جرول [Groll]، 2019؛ لارسون [Larson]، 2019). لقد اعترض هذا الاختراق البيانات التي كان بعضها بيانات طبيّة حساسة، والعائدة لثمانين مليون شخص (ويتاكِر [Whittaker]، 2019)، بمن فيهم حوالي نصف مجموع العمال الفيدراليين الأمريكيين (فريق بحث ثريت كونكت [ThreatConnect Research Team]، 2015). علاوةً على ذلك، وبحسب تقريرٍ صادرٍ عام 2019 (مجموعة جريفون العلمية وروديوم [Gryphon Scientific and Rhodium Group]، 2019) من إعداد لجنة المراجَعة الاقتصاديّة والأمنية الأمريكية–الصينية (U.S.–China Economic and Security Review Commission)، للصين أصلاً وصولٌ مباشرٌ إلى كميات كبيرة من البيانات السريرية والجينية الخاصة بسكّان أمريكيين من خلال استثمارات وشراكات مع شركات رعاية صحية أمريكية. وتواصل الصين أيضاً استراتيجية طويلة المدى لتصبح رائدة من حيث التكنولوجيا الحيوية (البيولوجية) وهي تتقدّم بسرعةٍ في المجال من خلال استثمار ثنائي الاتجاه مع شركات أمريكية، وشراكات في مجال الأبحاث مع مؤسسات أمريكية، وتوظيف علماء أجانب مولودين في الصين والذين تم تدريبهم في الولايات المتّحدة (مجموعة جريفون العلمية وروديوم [Gryphon Scientific and Rhodium Group]، 2019). قد تمكّن هذه الاستراتيجية الصين من زيادة موطئ قدمها في الوصول إلى بيانات الأمريكيين البيومترية، على مستوى الأفراد والمجموعات الفرعية على حدٍّ سواء،

إن باعتماد وسائل تجارية أو من خلال التجسّس.

وقد يزيد أيضاً نمو اعتماد إنترنت الأجسام المخاطر الجغرافية السياسية العالمية، لأن الدول التي تعتمد المراقَبَة الجماعيّة (surveillance states) قد تَسْتَخْدِم بيانات إنترنت الأجسام لتنفيذ أنظمة استبداديّة. فعلى سبيل المثال، تَسْتَخْدِم الصين بيانات الحمض الخلوي الصبغي (الحمض النووي) (DNA) في محاولةٍ لمراقبة الأيغور (Uighurs) (وي [Wee]، 2019). وقد أُفيد أيضاً بأنّ نظام الائتمان الاجتماعي في الصين (China's social credit scoring system) يَسْتَخْدِم كميات هائلة من البيانات المجمَّعَة، بما فيها السجلات الصحيّة، حول الأفراد من أجل تحديد جدارتهم وتحفيز السلوكيات المرجوَّة (مار [Marr]، 2019b). قد يزيد استخدام إنترنت الأجسام المنتشر على نطاقٍ واسعٍ خطر الضرر الجسدي، والتجسس، واستغلال البيانات من قبَل الخصوم.

المخاطر من حيث الأمن الإلكتروني

غالباً ما يتمّ تصنيف المخاطر من حيث الأمن الإلكتروني ضمن ثلاث فئات تُعرف بتسمية ثلاثي السريّة، والسلامة، والتوفّر (confidentiality, integrity, and availability *[CIA triad]*) (مركز أمن الإنترنت [Center for Internet Security]، غير مؤرَّخ). تعني السريّة أنّ الكيانات المصرَّح لها هي الوحيدة التي تطّلع على البيانات؛ وتعني السلامة أنّه لم يتم التلاعب بالبيانات التي تمّ جمْعها؛ ويعني التوفّر أنّه يتم الوصول إلى البيانات متى وحيث تدعو الحاجة إلى ذلك.

وفي وقتٍ مبكرٍ من عام 2019، لم تكن إدارة الغذاء والدواء (FDA) على علْم بأيّ إصابات أو وفيات ناتجة عن الهجوم الخبيث أو اعتراض الأجهزة الطبيّة المتّصلة (إدارة الغذاء والدواء [FDA]، 2019a).[9] على الرغم من ذلك، قد تتسبّب عرضياً نقاط الضعف في هذه الأجهزة بضرر جسديّ أو قد يتم استغلالها بشكلٍ خبيث من أجل التسبب بضرر أو بوفاة. فعلى سبيل المثال، تكمن نقطتا الضعف المشهورتان المتعلقتان بالأجهزة الطبيّة في أجهزة مزيل رجفان بُطين القلب ومضخّات الإنسولين المزروعة في الجسم، وهما ناتجتان عن سوء تنفيذ بروتوكولات الاتصال بين الجهاز وأنظمة الرصد عن بُعد. في الحالة الأولى، بَرَزَت نقطة ضعْف في برمجيات الاتصال اللاسلكيّ لجهاز مُقَوّم نُظُم القلب ومزيل رجفان بُطين القلب مزروع في الجسم وشائع (إدارة الغذاء والدواء [FDA]، 2019b). قد تُمَكِّن نقطة الضعف هذه مهاجماً ما من اعتراض الاتصال بين الجهاز المزروع في الجسم وأجهزة البرمجة السريرية أو آلات الرصْد المنزلي بطريقةٍ قد تتيح التلاعب بالبيانات أو إدخال أوامر خاطئة (خبيثة) للجهاز المزروع في الجسم. بالمثل، اكتَشَفَ باحثٌ أمنيّ عام 2016 ثلاث نقاط ضعْف في رمز الحاسوب لمِضخَّة إنسولين قد تتيح لمهاجمٍ ما ضخّ أوامر خبيثة، الأمر الذي يتسبب بضرر خطير (بيردسلي [Beardsley]، 2016).

بالإضافة إلى ذلك، ثمّة مخاوف مرتبطة بالنظام البيئي الأوسع نطاقاً حيث تُستَخدَم أجهزة إنترنت الأجسام (داس [Das]، زيدالي [Zeadally]، ووزيد [Wazid]، 2017). سيتّصل لاسلكياً جهازٌ جسديٌّ مزروعٌ في الجسم أو متّصل به بجهاز رصْد، على غرار هاتف أحدهم الذكي، والذي سينقل بعدئذٍ المعلومات ضمن خدمة سحابية. ويمكن بعد ذلك الوصول إلى البيانات من قِبَل طرفٍ خارجي، على غرار مُصنِّع الجهاز أو ممارس طبي. تُضيف هذه الكوكبة من المعدّات الحاسوبيّة والبرمجيات، ومسارات الاتصالات الجسديّة والمنطقية، والحدود التنظيمية طبقات متعددة من التعقيد والتي تكون عرضة للفشل، والتدهور، والاعتراض، والهجوم.

لقد بُذِلَت جهود لفهرسة نقاط الضعف المُكتَشَفَة في الأجهزة الطبيّة. يُصدِر فريق الجهوزية للطوارئ الإلكترونية المتعلقة بأنظمة المراقبة الصناعيّة (Industrial Control Systems Cyber Emergency Readiness Team [ICS-CERT])، وهو قسم تابع لوزارة الأمن الداخلي في الولايات المتحدة (Department of Homeland Security)، تحذيرات بشأن التهديدات المتعلّقة بالأجهزة الطبيّة. وتحتفظ ميدكريبت (Medcrypt)، وهي منظّمة غير ربحية للرعاية الصحية، بمستندٍ على الإنترنت يُعَدِّد كل واحد من هذه التحذيرات.[10] واعتباراً من يوليو/تموز 2019، كانت قد وثَّقَت 144 نقطة ضعْف فريدة تمّ اكتشافها منذ عام 2013،[11] وإنّ عدد نقاط الضعف آخذ بالازدياد،[12] بحسب ما يبيّنه الشكل رقم 2. إنّنا نتوقّع رؤية نموّ مستمرّ في تقارير نقاط ضعْف إنترنت الأجسام، وذلك لمجرّد أنّ الباحثين في مجال الأمن يبدأون بدراسة هذا المجال المتنامي.

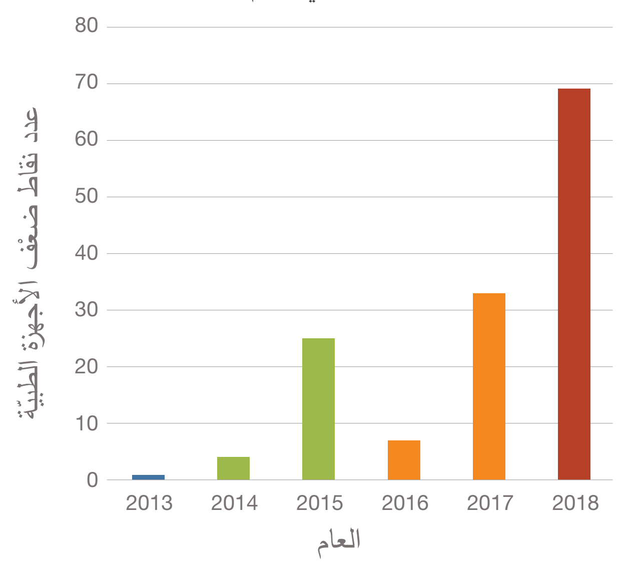
ومن بين نقاط الضعف المُحدَّدَة في هذه الأجهزة، تُعتبر أغلبيةٌ منها، أي 65 في المئة، عيوباً في المصادقة على المُستَخدِمين وشوائب على مستوى الرموز. قد تتيح العيوب على مستوى المصادَقَة للمُستخدِمين غير المصرَّح لهم الوصول إلى البيانات وربْطها (مثلاً، اعتراض سريّة الجهاز). وتشير الشوائب على مستوى الرموز إلى عيوبٍ في البرمجيات قد تتيح لمُستَخدِمٍ خبيثٍ اختراق سريّة النظام، أو سلامته، أو توفُّره. فعلى سبيل المثال، قد يتسبّب قرصانٌ إلكتروني بقيام الجهاز بتبادل البيانات مع مُستَخدِمين غير مُصرَّح لهم، أو بالتلاعب بالبيانات ليعمل الجهاز بشكلٍ خاطئ، أو بمجرّد وقْف عمل الجهاز.

تواجه أجهزة إنترنت الأجسام قضايا أمنيّة فريدة متعدّدة أخرى. وتشمل التوصيات التقليدية بشأن الأمن الإلكتروني تطبيق الرُقعة (التصحيح) (مثلاً، تثبيت رمز جديد لتصحيح الرمز المعيب)، وتطبيق العوامِل التخفيفيّة (مثلاً، تعطيل الخدمة المتأثِّرَة أو مكوّن البرمجيات المتأثِّر)، وتطبيق ضوابط أمنية إضافيّة على المكوّن الضعيف لإخفاء أي هجومٍ قادمٍ أو إعاقته بخلاف ذلك. على الرغم من ذلك، في حالات الأجهزة الصحيّة الشخصيّة التي يجوز زرْعها داخل جسم شخصٍ ما، والتي تتطلّب توفُّراً على مدار 24 ساعة وإلا قد لا تكون قابلة لتوفير الخدمة بأي طريقة عملية (مثلاً، إذا كان المريض يعيش في منطقةٍ نائيةٍ أو غير قادرٍ على زيارة منشأة صحيّة)، قد لا تكون العوامِل التخفيفيّة هذه مجدية أو حتّى ممكِنَة.

بالإضافة إلى الأمن الإلكتروني للأجهزة بحدّ ذاتها، يجب أن

الشكل رقم 2

نقاط ضعْف الأجهزة الطبيّة، في العام



المصدر: التحذيرات بشأن التهديدات الصادرة عن فريق الجهوزية للطوارئ الإلكترونية المتعلقة بأنظمة المراقبة الصناعيّة (ICS–CERT). يُصدِر فريق الجهوزية للطوارئ الإلكترونية المتعلقة بأنظمة المراقبة الصناعيّة (Industrial Control Systems Cyber Emergency Readiness Team [ICS–CERT])، وهو قسم تابع لوزارة الأمن الداخلي في الولايات المتحدة (Department of Homeland Security)، تحذيرات بشأن التهديدات المتعلّقة بالأجهزة الطبيّة.

يكون أيضاً للمستودعات التي تُخزِّن بيانات المُستَخدِمين ضوابط كافية من حيث الأمن، والبرمجيات، والسلامة. فإنْ لم يكن الأمر كذلك، قد يكون المُستَخدِمون بخطر، بحسب ما وَضَّحَه الاعتماد السريع للسجلات الصحيّة الإلكترونية (EHRs). كان الهدف من قانون علاجات القرن الحادي والعشرين الصادر عام 2016 (The 21st Century Cures Act of 2016) معالَجَة الصعوبات التي اقترَن بها اعتماد السجلات الصحيّة الإلكترونيّة من خلال تحسين قابلية التشغيل المتبادَل لنظام المعلومات الصحيّة ووصول المرضى إلى البيانات. وعلى الرغم من هذا التشريع، تَسَبَّبَت السجلات الصحية الإلكترونيّة التي كانت مُصمَّمة إلى حدٍّ كبيرٍ للحدّ من الأخطاء الطبيّة، في آلاف حالات الوفاة، أو الإصابات أو الحوادث الوشيكة لدى المرضى بسبب عيوب البرمجيات، أو خطأ المُستَخدِم، أو قضايا أخرى (شولت [Schulte] وفراي [Fry]، 2019a).

قد يكون هناك أيضاً مفاضلات أساسيّة بين الأمن وقابلية الاستخدام بالنسبة إلى أجهزة إنترنت الأجسام. أنظُر مثلاً في مِضخَّة إنسولين متّصلة. فقد تقترح الممارسات الفضلى في مجال الأمن أن يتمّ حصْر الوصول إلى الجهاز بهؤلاء الذين يملكون تصريحاً ملائماً لإصدار الحقنات أو تعديلها فحسب، وهو أمر غالباً ما يجري من خلال أسماء مُستخدِمين وكلمات مرور أو عبر تسجيل دخول بيومتري. على الرغم من ذلك، لن يتسنّى على الأرجح لمريضٍ يعاني من صدمة إنسولين (insulin shock) الوقت أو لن تتوفّر له القدرات العقلية لإدخال معلومات حول هويته أو هويتها في الجهاز. ولكن قد تؤدي سهولة الاستخدام إلى طرق مُختَصَرَة بالنسبة إلى الأمن الإلكتروني، وقد تهدد الطرق المُختَصَرَة هذه الخصوصيّة.

البيانات والمخاطر من حيث الخصوصية

تُغذّي البيانات الخوارزميات التي تخدم إعلانات هادِفة، وتقيِّم الخطر الائتماني أو غيره من المخاطر، وتدفع بجزءٍ كبيرٍ من اقتصاد الإنترنت. تجمع أجهزة إنترنت الأجسام (IoB) معلومات شخصية إلى حدٍّ كبيرٍ وتخزّنها، وهي بحسب ما يُزعَم أكثر حميميّةً من أي نوع آخر من معلومات المُستَخدِمين، وبالتالي تكثُر المخاطر من حيث الخصوصيّة والسريّة. ويمكن تسجيل معلومات حول أماكن تواجد المُستَخدِمين، ووظائفهم الجسدية، والأمور التي يرونها ويسمعونها وحتّى يفكّرون بها، وتخزينها.

ثمّة مسائل متعددة لم يتم حلُّها بشأن مَن يملك السلطة لاستخدام البيانات التي تَجْمَعُها أجهزة إنترنت الأجسام، وطريقة استخدامها. فعلى سبيل المثال، ثمّة مسائل حول الأمور التي يمكن أن يحققها إنفاذ القانون بالنسبة إلى معلومات إنترنت الأجسام، وحول ما إذا كان هذا الاستخدام يشكّل انتهاكاً لمبادئ الحماية من التفتيش والحجز غير القانونيين أو تجريم الذات التي يكفلها التعديلان الرابع والخامس للدستور الأمريكي (4th and 5th Amendments to the U.S. Constitution). كان يتم أصلاً استخدام المعلومات الطبية، على غرار بيانات مُنَظِّم ضربات القلب، لاتهّام أشخاصٍ بجرائم (ووتسون [Wootson]، 2017). وتم الإعراب عن مخاوف حول كيفية استخدام الشرطة للبيانات الخاضِعة لإدارة مراكز دمْج البيانات المملوكة والمُشغَّلَة من قبَل الدولة، والتي تجمع بيانات شخصية، بما فيها بيانات صحيّة، وتحلّلها من مصادر عامّة وخاصّة متعدّدة (هاسكينز [Haskins]، 2019). وبحسب تحليل دليل المُستَخدِم التابع لمركز دمج، يتمّ "تجميع المعلومات من مصادر متنوعة وتوليفها بطريقةٍ تمنح السلطات المعنيّة بإنفاذ القانون معرفةً شبه كاملة حول أي مُشتبَه به تُقَرّر مراقبته" (هاسكينز [Haskins]، 2019). وقد يكون لبلدان أخرى وصولٌ مماثلٌ إلى معلومات الأشخاص الشخصيّة وقد تنخرط مع الولايات المتّحدة بمعاملةٍ بالمثل من حيث البيانات (أي تبادلها) (إدارة إنفاذ قوانين الهجرة والجمارك في الولايات المتحدة [U.S. Immigration and Customs Enforcement]، غير مؤرَّخ).

قد يهدّد جمْع البيانات خصوصيّة مُستَخدِمي إنترنت الأجسام في حال عدم تطبيق ضمانات للحماية من سوء الاستخدام. فقد تُشكّل عملية الجمْع بحدّ ذاتها، بما فيها أي بيانات يتمّ جمْعها، وتواتر جمْعها، وما إذا تمّ الحصول على الموافقة المستنيرة (لا سيّما في صفوف المجموعات الضعيفة مثل الأشخاص القاصرين أو المسجونين)، وما إذا كان باستطاعة المُستَخدِم أن يختار وقْف جمْع البيانات أو إعادة بيعْها في أي وقت، خطراً كامناً على الخصوصيّة.

يبدو أن مُستهلِكي إنترنت الأجسام قد أقرّوا بالحاجة إلى توفير بياناتهم إلى مُطوِّرين أو آخرين لاستخدام أحد منتجات إنترنت الأجسام. على الرغم من ذلك، ليس من الواضح ما إذا شَرَع المستهلِكون انطلاقاً من معرفةٍ كاملةٍ بخصوص كيفيّة جمْع البيانات وإمكانية استخدامها. فقد بيّن تحقيقٌ حول آلات الضغط الإيجابي المستمرّ في المجرى الهوائي (continuous positive airway

pressure [CPAP]) المُستَخدَمَة من قِبَل أولئك الذين يعانون من انقطاع النفس الانسدادي النومي (sleep apnea)، أنّه كان يتم إرسال بيانات المرضى إلى شركات التأمين بدون معرفة المُستَخدِمين لرصْد التزامهم (آلِن [Allen]، 2018a). في حال لم يستخدِم المرضى آلة الضغط الإيجابي المستمرّ في المجرى الهوائي للفترة الزمنية المطلوبة، ترفض شركة التأمين تغطية التكاليف.

قد تكون المعلومات التي تكشف عن عادات نمط عيش غير سليم أدَّت أصلاً إلى رفْع أقساط التأمين الصحيّ بالنسبة إلى بعض الأشخاص (آلِن [Allen]، 2018b). وقد تؤدّي زيادةٌ في أجهزة إنترنت الأجسام إلى تصعيد هذا الاتّجاه المُتَمَثِّل بالجمْع بين البيانات الصحيّة والتفاصيل الشخصية الأخرى، والتي يجمعها وسطاء البيانات، وهم كناية عن شركات لا تربطها علاقة مباشرة بالعملاء وإنّما تشتري معلوماتهم الشخصية وتبيعها، لزيادة أقساط التأمين أو الحدّ من الوصول إلى الرعاية.

وتُطرَح مسألة الحقوق الطبيعيّة التي قد يحقّ لمُستَخدِمٍ ما التمتّع بها. فعلى سبيل المثال، هل يجب أن يكون لمُستَخدِمٍ ما الحقّ في إلغاء الاشتراك إمّا بالنسبة إلى أنواع معيّنة من جمْع البيانات أو تخزينها؟ وهل يجب على الولايات المتّحدة إنفاذ حقّ في النسيان بالنسبة إلى أولئك الذين يطلبون مسْح بياناتهم؟[13] يجادل النقّاد بأنّ الحقّ في النسيان قد يؤثّر على حريّة التعبير، (بُوْكوت [Bowcott]، 2018)، أو يسمح بقيام سجلٍّ عامٍ غير كامل ("القضية ضدّ الحقّ في النسيان" The Case Against a Right to Be"] Forgotten"]، 2018)، أو بإعادة كتابة التاريخ من قِبَل الأنظمة الاستبداديّة (سويرِنجِن [Swearingen]، 2019). وتتمثّل مسألة أخرى بالحقّ في الخصوصيّة بعْد الوفاة، أي ما أن يموت شخصٌ ما، هل يجب حذْف البيانات بشكلٍ نهائيّ، أو هل يجب أن تكون متوفرّة ليصل إليها الأقرباء؟[14] قد يشكّل ذلك قضيّةً حساسةً بوجهٍ خاص في حال الانتحار، أو القتل الرحيم، أو مراقبة الجنين.

وبالإضافة إلى ذلك، قد يكون تفسير بيانات إنترنت الأجسام ومُخرجات الخوارزميات التي تعتمد على تلك البيانات منحازةً أو مُضِرّة بخلاف ذلك للمُستَخدِم، لا سيّما إذا كانت تلك العمليات تقترن بمستوى محدود من الشفافية (أوسوبا [Osoba] ووِلسِر [Welser]، 2017).

تبرز أيضاً مخاوف بشأن تحمُّل البيانات، ما يعني أن النتائج المستخلَصَة من مجموعة اختبارات جينية أو استخدام جهاز طبي معين لإنترنت الأجسام قد يحدّد أحداً على أنّه يحمل مرض جيني يمكن أن ينتقل إلى أولاده أو أولادها، الأمر الذي قد يؤدي يوماً ما إلى حرمان هؤلاء الأطفال من تأمينٍ معيّنٍ أو من منافع أخرى (كليتزمان [Klitzman]، 2012).

وأخيراً، لا وجود حتّى الآن لمعايير قانونيّة حول الشخص الذي يملك البيانات المولَّدَة من أي جهاز إنترنت أجسام معيّن، فهل هو المُستَخدِم، أو المُصنِّع، أو الجهة المزوِّدَة للرعاية الصحية؟ فقد شكّلَت ملكية البيانات قضيةً قائمةً منذ وقتٍ طويلٍ في الرعاية الصحية (مينغاست [Meingast]، روستا [Roosta]، وساستري [Sastry]، 2006). وتدرس شركات استشارات الأعمال كيفية تسييل بيانات إنترنت الأجسام بالطريقة الفضلى (ديتشمان وآخرون [Deichmann et al.]، 2016؛ روسو [Russo] وألبِرت [Albert]، 2018). وتُعتَبَر السياسات التي تُنَظِّم بيع معلومات المُستَخدِمين لوسطاء البيانات من الأطراف الثالثة أو التي تنظِّم كيفيّة عَمَل وسطاء البيانات ناشئة، إنْ لم تكن غير متوفّرة إطلاقاً (ماكميلِن [MacMillan]، 2019).

الاعتبارات الأخلاقية

قد تُعتبر مخاطر متعدّدةٌ من بين تلك التي تمت مناقشتها سابقاً أخلاقيةً بطبيعتها باعتبار أنّها تعكس قِيَماً كامِنة بالنسبة إلى الأمن والخصوصيّة. ولكن، يجب علينا أيضاً النظر في التداعيات الضارّة المحتمَلَة لإنترنت الأجسام (IoB) بالنسبة إلى قِيَمٍ أخرى مهمّة للأمريكيين، على غرار العدالة والاستقلالية الذاتيّة.

نتائجُ غير عادِلَة

يتمثّل أحد المنافع الموعودة لتكنولوجيات إنترنت الأجسام (IoB) بالحدّ من التباينات في نتائج الرعاية الصحية الأمريكية من خلال جعْل الرعاية الوقائيّة والتشخيصيّة أقلّ كلفةً وأسهل للوصول إليها، ولكنّه ليس من الواضح ما إذا كانت هذه التكنولوجيات ستحدّ من تكاليف الرعاية الصحيّة أو سيكون من الممكن الوصول إليها بسهولة بالنسبة إلى عموم الشعب.

بالإجمال، ساهَمَت التكنولوجيات المتقدِّمة في مجال الرعاية الصحيّة في زيادةٍ في التكاليف الإجماليّة (كالاهان [Callahan]، 2008). وقد تتفاقَم التباينات بسبب العوائق في وجه الوصول إلى الصحّة الرقمية (digital health) والصحّة عن بُعْد (telehealth) بالنسبة إلى أولئك الذين لا يملكون وصولاً موثوقاً إلى الإنترنت (غونزاليس [Gonzales]، 2017. ولا يستطيع أشخاصٌ متعدّدون من أولئك الذين لا يملكون تأميناً الوصول إلى تكنولوجيات الرعاية الصحيّة المتقدِّمة. وحتّى بالنسبة إلى الأشخاص المؤمَّنين، قد لا توفِّر الجهات المزوِّدَة التغطية لإنترنت الأجسام المتطوّر إلى حين وما لمْ يبيّن تحليل المنافع بالمقارنة مع التكاليف أن هذه الأجهزة تُحسِّن بالفعل النتائج الطبية على المديَيْن القصير والطويل بشكلٍ يتناسب مع تكاليفها. سيتطلّب هذا الأمر أدلّةً كبيرة، وسيكون من المهمّ معرفة ما إذا كانت هذه المنافع تتراكم على امتداد شرائح متعدّدة من السكّان (مثلاً، المرضى الكبار في السنّ الذين قد يكونوا أقلّ معرفةً من الناحية التكنولوجية، والمجموعات ذات الوضع الاجتماعي الاقتصادي المتدني، وما إلى هنالك).

بالإضافة إلى ذلك، تُعْتَبَر البيانات الطبيّة ضعيفةً في وجْه التحيُّز من حيث المُدخلات، حيث أنّ مُستَخدِمي أجهزة إنترنت الأجسام النموذجيين هم مجموعة مُختارَة ذاتياً. قليلةٌ هي الأمور المعلومة عن أولئك الذين لا يستخدِمون أجهزة إنترنت الأجسام، إنْ بشكلٍ اختياريٍ أو بسبب الكلفة أو عوائق أخرى في وجه الوصول.

ويُشكِّل عدم تمثيل البيانات الصحيّة مُشكلةً موثّقةً بشكلٍ جيّد، لأنّه يتمّ عادةً جمْع أغلبية البيانات السريريّة بشأن المُشارِكين الذكور، ذوي الأصل الأوروبي، الأصغر سنّاً ومن الطبقتين الوسطى والعليا (كابْلان [Caplan]، وفريسِن [Friesen]، 2017). وعلى الرغم من قانون إعادة تنشيط حوكمة المنظّمات غير الربحيّة الصادر عام 1993 (Revitalization Act 1993) الذي ينصّ على إجراء تجارب سريريّة بتمويلٍ من المعاهد الوطنية للصحّة (National Institutes of Health) لتشمل النساء والأقليّات، لم يتم تحقيق تقدُّم كبير (جيلِر وآخرون [Geller et al.]، 2018، 2011). ليست البيانات الصحيّة الواسعة النطاق، على الرغم من أنّها مُستَمَدّة من مجموعات من العالَم الحقيقيّ، مُحصَّنَةً في وجه التحيّزات من حيث المُدخلات؛ إذ تنطوي بيانات السجلات الصحيّة الإلكترونيّة (EHRs) والمطالبات على مرضى مُنخرطين بشكلٍ نشط في أنظمة الرعاية الصحيّة، ما يؤدي إلى عيّنات هي بالإجمال أكثر مرضاً أو أكثر إعاقةً من عموم الشعب (أجنييل [Agniel]، كوهان [Kohane]، وويبِر [Weber]، 2018؛ فيرهيج وآخرون [Verheij et al.]، 2018؛ شنيويس [Schneeweiss] وأفورن [Avorn]، 2005). قد تَتَجَنَّب البيانات الصحيّة المولَّدَة من الشخص (PGHD) التي يتمّ جمْعها من عملاء خارج العيادة بعض هذه الانحيازات وإنّما تتطلّب اعتبارات أخرى من حيث أخْذ العيّنات والغائبَة إلى حدٍّ كبيرٍ من الدراسات السابقة.

الحريّة من إنترنت الأجسام (IoB)

في الوقت الذي يصبح فيه إنترنت الأجسام (IoB) أكثر انتشاراً على نطاق واسع، قد يبرز ضغطٌ جسديٌّ أو نفسيٌّ متزايدٌ على أولئك الذين يريدون أن يعيشوا حياتهم بحدٍّ أدنى من الاعتماد على هذه الأجهزة أو التفاعل معها. قد يَجْمَع بعض تكنولوجيات إنترنت الأجسام معلوماتٍ حساسةً بشكلٍ محتمل بما يتجاوز الشخص الذي يرتدي الجهاز أو مالكه بحد ذاته. فعلى سبيل المثال، إنّ أجهزة الواقع المُعزَّز (augmented reality devices) أو أجهزة السمع "الذكية" المزروعة في الجسم ("smart" hearing implants) مصمّمةٌ لتسجيل مقاطع الفيديو والمقاطع الصوتية. قد يؤدي ذلك إلى بروز قلق بشأن الخصوصيّة من جانب الأشخاص الذين تتم رؤيتهم أو يتم سماعهم من خلال هذه الأجهزة ولكن لم يوافقوا على أن يتم جمْع صورهم أو أصواتهم. وكان مثلٌ حول هذه الظاهرة التفاعل مع نظام الواقع المُعزّز جوجل جلاس (Google Glass augmented reality system) الذي ولَّد صرخةً عامّة، والمُوَضَّحَة بدقّة في حركة "أوقفوا السايبورغات" (Stop the "Cyborgs") (فاريفار [Farivar]، 2013). لقد أدّى استخدام أنظمة التعرّف إلى الوجه (face recognition systems) من قِبل السلطات المعنية بإنفاذ القانون إلى انتقادٍ مفاده أنّ الأنظمة منحازَة، وأنّه يتم استخدامها أيضاً لتصنيف الأشخاص بدون موافقتهم وبناءً على فهْم محدود لكيفية استخدام المعلومات (أكسون أيه.آي [Axon A.I.] ومجلس أخلاقيات تكنولوجيا حفْظ الأمن والنظام العام [Policing Technology Ethics Board]، 2019). وتنطبق انتقادات مماثلة على إنترنت الأجسام المُجهَّز بكاميرات وأدوات أخرى يمكن استخدامُها لتسجيل أشخاص أو لتحديد هويتهم.

لقد سعى بعض المنظّمات إلى استخدام إنترنت الأجسام من أجل إدارة الموظفين. ففي حين قد تُعْتَبَر شارات الموظّفين المُستَخدَمَة للوصول إلى مكان العمل من أجهزة إنترنت الأجسام، ثمّة تمييز بين الرصد مع تغذيةٍ راجعةٍ سلبيّة (مثلاً، يُصْدِر جهاز قراءة الشارات صوت تنبيهي ويفتح قفْل باب المبنى للسماح بالدخول) والرصْد مع تغذيةٍ راجِعةٍ مُتصلّة بالشبكة (مثلاً، يستمرّ الجهاز بتتبّع أماكن تواجد المستَخدِم بشكلٍ متواصل). وقد سَجَّلَت شركة أمازون (Amazon) براءة اختراع لتكنولوجيّات شريطٍ يوضَع على معصم اليد ويمكنه تتبُّع سلوك الموظّفين، وهو يهتزّ لتشجيعهم على تحقيق إنتاجية أكبر (سولون [Solon]، 2018). وتسعى تكنولوجيات أخرى إلى تحديد الحالات التي يشعر فيها العمّال بالنعاس أو يتشتت انتباههم (ديروسو [Derousseau]، 2017). كما يقوم الباحثون باختراع أجهزةٍ يمكن ارتداؤها تتتبَّع بحسب ما يُدَّعى أداء موظّفٍ ما في مكان العمل (مثلاً، الفترة الزمنية التي يقضيها في العمل، وفترات الاستراحة من العمل، والنشاط الجسديّ، ومستويات النعاس) بدقّة تساوي حوالي 80 في المئة (هولي [Holley]، 2019). قد تُفيد هذه القدرات أصحاب العمل وتجعلهم أكثر دفْعاً من البيانات وأكثر فعاليّة (ناك وآخرون [Knack et al.]، 2019)، وإنّما قد تؤدي إلى نفور العمّال وتضرّ بالاحتفاظ بهم في حال اعتبرها الموظفون تدخّليةً وغير ضروريّة.

من الأكثر ترجيحاً أن يجري الاعتماد القسري لتكنولوجيا إنترنت الأجسام في نظام العدالة الجنائيّة. فقد تضغط المحاكم، أو السجون أو مكاتب إخلاء السبيل على الأشخاص لاستخدام أجهزة إنترنت الأجسام أو تطلب منهم ذلك. وتستخدِم ولايات قضائية متعددة أساور إنترنت الأجسام التي توضَع على الكاحل (IoB ankle bracelets) لمنْع الذين ينتظرون المحاكمة من الفرار. وحتّى وإنْ وافق الأشخاص المسجونون، فهم قد يكونوا غير مدركين للمخاطر المحتَمَلة. فقد يتخيّل أحدهم أن تحلّ علاجات إنترنت الأجسام الشبيهة بحبّة أريبيبرازول رقميّة، والمُستَخدَمَة لعلاج اضطرابات نفسيّة، محلّ العلاج النفسي التقليدي الذي تأمر به المحاكم. وقد تتمثّل متطلّباتٌ موسَّعَةٌ أخرى بالنسبة إلى أولئك الذين تمّ توقيفهم أو تمّت إدانتهم بجرائم باستخدام إنترنت الأجسام من أجل رصْد موقعهم، أو صحّتهم، أو استهلاكهم للكحول أو المخدرات، أو مؤشرات أخرى للسلوك المُتَصَوَّر غير المرغوب به اجتماعياً.

استقلالية الجسم وسلامته

يرتبط اعتبارٌ أخلاقيٌّ آخر بحقوق المستَخدِمين بشأن التكنولوجيات التي يتمّ دمْجها في أجسادهم. على الرغم من ذلك، يتضارب بشكلٍ محتمل حقّ المُستَخدِمين هذا مع محاولات مطوِّري التكنولوجيات للاحتفاظ بالحقوق من حيث البرمجيات والأجهزة. ويتمثّل أحد الأمثلة حول هذا التضارب باتفاقيات ترخيص المستخدِمين النهائيين

(end-user license agreements [EULAs]) التي يستَخدِمها مُطَوِّرو البرمجيات للحدّ من الأمور التي يستطيع مُستَخدِمٌ ما القيام بها للبرمجيات بعْد الشراء. قد تقيّد اتفاقية ترخيص المستخدِم النهائي إجراء التعديلات على البرمجيات أو تقيِّد استخدامها لضمان الأداء المقصود أو لحماية الملكية الفكرية. على الرغم من ذلك، ما أن يتمّ زرْع جهازٍ ما في جسم شخص، قد يصبح استمرار تحكُّم المطوِّر بالأجهزة بفعْل ملكيتها إشكالياً (ماتويشين [Matwyshyn]، 2018؛ ماتويشين [Matwyshyn]، 2019، المجلس الأطلسي [Atlantic Coucnil]، 2017، المؤتمرات الدولية حول الحواسيب، والخصوصيّة وحماية البيانات [CPDP conferences]، 2018؛ كليّة إدنبرغ للحقوق [Edinburgh Law School]، 2018، 26:28-28:08). فعلى سبيل المثال، ماذا إنْ حاول مُطوِّرٌ ما فرْض اتفاقيّةٍ لتغيير سياسات استخدام البيانات المتعلّقة بجهازٍ تمّ زرْعه في الجسم أصلاً (وربّما بشكلٍ دائم)؟ سيجادل البعض أنّ للناس حقّ معنويّ أساسيّ في الاستقلالية الجسديّة وأنّ هذا الحق يجب أن يُمَكِّنهم من التحكُّم بشكلٍ كامل بأجهزتهم باعتبارها امتداداً لأجسامهم.[15] وبقدر ما يَعْتَبر المُستَخدِمون الجهاز جزءاً من جسمهم، قد يعتقدون بشكلٍ معقول أنّه يحقّ لهم مقاومة التغييرات المفروضة من المطوِّر. وقد يُصِرّون أيضاً على القدرة على تعديل الجهاز حسبما يرونه مناسباً. ثمّة أصلاً أمثلة حول قيام مستخدِمين "بكسْر حماية" (jailbreaking) أجهزةِ إنترنت الأجسام أو قَرْصَنَتها إلكترونياً من أجل تحسين عملها (براون [Brown]، 2019؛ هورلي [Hurley]، 2014). على الرغم من ذلك، أحبط المطوِّرون هذه التعديلات، مُجادِلين أنّها قد تؤثّر سلباً على عمل الجهاز (زهانغ [Zhang]، 2019).

إنّ بعض أنواع إنترنت الأجسام غير منظّمٍ إلى حدٍّ كبير، مثل الرقاقات البيولوجيّة للتعرّف بالترددات اللاسلكيّة (RFID bio-chips) أو تكنولوجيا تتبُّع الصحّة (health-tracking technology). ولكن قد تدعو الحاجة في المستقبل إلى تنظيم الأحكام والشروط التي يمكن استخدام تكنولوجيات إنترنت الأجسام بموجبها والنظر في وسائل الحماية بالنسبة إلى بعض المجموعات الضعيفة، لا سيّما لضمان تحلّي المُستخدِمين بحقوق بشأن التكنولوجيات المزروعة في أجسامهم.

حوكمة أجهزة إنترنت الأجسام (IoB) والمعلومات

كما هي الحال بالنسبة إلى أغلبية المنتجات الاستهلاكية في الولايات المتّحدة، تتمّ إدارة حوكمة أجهزة إنترنت الأجسام (IoB) من خلال مجموعةٍ من الوكالات الحكوميّة والفيدراليّة المباشرة وغير المباشرة، والمنظّمات غير الربحيّة، ومجموعات تأييد المستهلِكين. فعلى سبيل المثال، يتمّ إرسال إشعارات سحْب المنتجات من قِبَل إدارة الغذاء والدواء (FDA) (إدارة الغذاء والدواء [FDA]، 2018c) ولجنة سلامة المنتجات الاستهلاكية (Consumer Product Safety Commission) (لجنة سلامة المنتجات الاستهلاكية في الولايات المتحدة [U.S. Consumer Product Safety Commission]، 2018) على حدٍّ سواء. وتساعد لجنة التجارة الفيدراليّة (Federal Trade Commission [FTC]) في معالَجَة أمن إنترنت الأشياء (لجنة التجارة الفيدرالية [FTC]، 2015) وعمليات اختراق البيانات الصحيّة (لجنة التجارة الفيدرالية [FTC]، 2010)، ويؤثّر المعهد الوطني للمعايير والتكنولوجيا (National Institute of Standards and Technology [NIST]) على الأمن الإلكتروني المدني والحكومي على حدٍّ سواء، ويضطلع بنشاطٍ مرتبطٍ بإنترنت الأشياء (IoT) (المعهد الوطني للمعايير والتكنولوجيا [NIST]، 2019) وبالأنظمة الجسديّة الإلكترونيّة (مجموعة العمل العامّة المعنيّة بالأنظمة الجسديّة الإلكترونيّة والتابعة للمعهد الوطني للمعايير والتكنولوجيا [NIST Cyber Physical Systems Public Working Group]، 2016). إنّنا في هذه الدراسة لا نستكشف كل منظّمة بشكلٍ معمّقٍ وإنّما نقدّم لمحة عامّة حول التأثيرات الرئيسيّة للحوكمة فيما يتعلّق بأمن أجهزة إنترنت الأجسام وخصوصيتها. وبشكلٍ أكثر تحديداً، إنّنا نميّز بين اللوائح التي تنطبق على جهاز إنترنت الأجسام بحدّ ذاته واللوائح التي تنطبق على المعلومات التي يتمّ جمْعها، أو تخزينها أو نقْلها من قِبَل الجهاز. وعلى الرغم من الجهود المبذولة لتنظيم إنترنت الأجسام، يمرّ عددٌ من هذه الأجهزة والمعلومات التي تَجْمَعها بدون تدقيقٍ تنظيمي.

حوكمة أجهزة إنترنت الأجسام (IoB)

إنّ الكيانيْن الأوليَيْن المسؤوليْن عن حوكمة أجهزة إنترنت الأجسام (IoB) (إنّنا نعالج المعلومات التي تَجْمَعها أجهزة إنترنت الأجسام في القسم التالي) هما إدارة الغذاء والدواء (FDA) ووزارة التجارة الأمريكية (U.S. Department of Commerce).[16]

جهود إدارة الغذاء والدواء (FDA)

إنّ إدارة الغذاء والدواء (FDA)، وهي جزءٌ من وزارة الصحة والخدمات البشرية الأمريكية (U.S Department of Health and Human Services)، مسؤولةٌ عن سلامة الأجهزة الطبية. وأملاً بتعزيز الابتكار في مجال الصحّة الرقمية، طوَّرَت إدارة الغذاء والدواء خطّة عمل بشأن الابتكار في مجال الصحّة الرقمية (Digital Health Innovation Action Plan). على الرغم من ذلك، يستبعد قانون علاجات القرن الحادي والعشرين (The 21st Century Cures Act) الوكالة من تولّي الولاية القضائيّة بشأن الأجهزة الصحيّة الإلكترونيّة (EHRs). وقد دعا رئيس إدارة الغذاء والدواء السابق سكوت غوتليب (Former FDA Chief Scott Gottlieb) الكونغرس لسنّ لوائح أكثر صرامةً ترعى السجلات الصحيّة الإلكترونيّة ولتحديد الحالات التي قد يستدعي فيها السجل الرقمي لمريضٍ ما رقابةً حكوميّة (شولت [Schulte] وفراي [Fry]، 2019b).

بالنسبة إلى تكنولوجيات إنترنت الأجسام (IoB) التي تخضع لرقابة إدارة الغذاء والدواء لكونها أجهزةً طبيّة، تعزّز إدارة الغذاء والدواء وسائل الحماية المتعلقة بالأمن الإلكتروني من خلال مقاربةٍ توزِّع المسؤولية بين أصحاب الشأن المختلفين. وتتشارك الوكالة أيضاً مع قراصنة إلكترونيين وشركاتٍ متخصصة في الأجهزة الطبيّة، مثل قرية القرصنة البيولوجية الإلكترونية التابعة لديفكون (DEFCON's Biohacking Village)، لتحديد نقاط ضعْف الأجهزة الطبيّة والكشْف عنها. وترأسَت إدارة الغذاء والدواء ومجموعات تأييد خاصّة حملات متعدّدة لتقييم سلامة الأجهزة الطبية المزروعة في الجسم والمتصلّة وحمايتها بشكل أفضل. فعلى سبيل المثال، عَقَدَت إدارة الغذاء والدواء منذ عام 2013 ورش عمل عامّة متعدّدة مُصمَّمَة للحصول على الإرشاد، والمعايير والممارسات الفضلى بالنسبة إلى أمن الأجهزة الطبية الإلكتروني ومراجَعتها (إدارة الغذاء والدواء [FDA]، 2019c). وقد أصدَرَت أيضاً وثائق إرشاديّة ما قبْل طرْح المنتجات في السوق وما بعْده في محاولةٍ لمساعَدَة مُصنّعي الأجهزة على فهْم كيفية تحديد التهديدات من حيث الأمن الإلكتروني ونقاط الضعف في منتجاتهم والتخفيف منها (إدارة الغذاء والدواء [FDA]، 2018d؛ إدارة الغذاء والدواء [FDA]، 2016؛ إدارة الغذاء والدواء [FDA]، 2005). توفّر هذه الوثائق إرشاداً غير ملزِمٍ لكيف يمكن أن تلتزم جهة مُصنِّعَة لجهازٍ ما باللوائح الصادرة عن إدارة الغذاء والدواء من أجل سلامة المرضى.

وتنشر إدارة الغذاء والدواء أيضاً إشعارات استشاريّة حول نقاط الضعْف المعروفة في الأجهزة الطبية الأساسيّة وتدعم قائمةً لتوزيع البريد الإلكتروني تُحذِّر المُستخدِمين لدى العلْم بقضايا (إدارة الغذاء والدواء [FDA]، 2019a). وتم أيضاً بذْل جهودٍ لتبادل المعلومات مع مراكز تبادل المعلومات الصحيّة وتحليلها (health information sharing analysis centers [H–ISAC]) لتسهيل تبادُل المعلومات المرتبطة بالأمن الإلكتروني بين الجهات المُزوِّدَة للرعاية الصحيّة والمُصنِّعين. ويساعد هذان الجهدان على تعزيز التوعية حول المعلومات وشفافيتها بالنسبة إلى المُستهلِكين وغيرهم من الممارسين، وقد يساعدان على المدى الطويل على تحسين الأمن الإجمالي لهذه الأجهزة، على الرغم من عدم وجود دليلٍ على هذا الأمر حتّى الآن.

وبالإضافة إلى ذلك، تعمل إدارة الغذاء والدواء مع مؤسسة ميتر (MITRE Corporation) لتطوير نظام درجاتٍ تقييميّ مُصَمَّمٍ لترتيب خطورة نقاط ضعْف البرمجيات في الأجهزة الطبيّة (تشايز [Chase] وكولي [Coley]، 2019). وفي حين يوجد أصلاً معيارٌ صناعيٌّ لتقييم درجة نقاط ضعْف البرمجيات في أنظمة حاسوبيّة أكثر تقليدية (راجِع نظام الدرجات التقييمي لنقاط الضعف الشائعة "سيج" [Common Vulnerability Scoring System SIG]، غير مؤرَّخ)، إنّه أداة مباشرة ولا يعالج بشكلٍ ملائمٍ التأثيرات المحتمَلَة على الصحة والسلامة بالنسبة إلى مريضٍ تمّت قرصنة جهازه الطبي إلكترونياً. وسيضمن هذا المشروع تمكُّن المُصنِّعين ومقدّمي الرعاية من تقييم خطر نقاط الضعف وترتيبها بحسب الأوّلوية بفعالية أكبر.

وعلى الرغم من أنّ إدارة الغذاء والدواء تحقّق خطوات كبيرة في مجال أمن الأجهزة الطبية الإلكتروني، لا يدخل عدد من أجهزة إنترنت الأجسام، ولا سيّما تلك المتوفِّرَة للاستخدام الاستهلاكي، ضمن نطاق الولاية القضائية لإدارة الغذاء والدواء.

الجهود الأخرى

لقد بدأ مسؤولون فيدراليون وحكوميّون بمعالَجَة مخاطر الأمن الإلكتروني المرتبطة بإنترنت الأجسام (IoB) والتي تخرج عن نطاق رقابة إدارة الغذاء والدواء (FDA)، ولكن ثمّة قوانين قليلة تفرض ممارساتٍ فضلى في مجال الأمن الإلكتروني. إنّ كاليفورنيا هي الولاية الأولى التي سنَّت قانوناً يرعى حماية إنترنت الأشياء (IoT)، وهو القانون رقم SB–327، الذي دَخَل حيز التنفيذ في يناير/كانون الثاني 2020. وينصّ قانون كاليفورنيا على أنّه يتوجّب على "مُصنِّع جهازٍ متّصل ... أن يجهِّز الجهاز بميزة أو ميزات أمنيّة معقولة تكون ملائمة لطبيعة الجهاز ووظيفته." فعلى سبيل المثال، إنّه يحدّد أنّه قد لا تكون لأجهزة إنترنت الأشياء كلمات مرور افتراضيّة عامّة. وقد ناقَشَت ولايات أخرى تشريعاتٍ بشأن أمن إنترنت الأشياء ولكنّها لم تمرر القوانين. ففي مارس/آذار 2019، أعادت مجموعة من أعضاء مجلس الشيوخ من الحزبين إدخال قانون تحسين الأمن الإلكتروني لإنترنت الأشياء لعام 2019 (Internet of Things Cybersecurity Improvement Act of 2019)، الذي يحاول تحسين الأمن من خلال توثيق الممارسات الفضلى لتطوير أجهزة إنترنت الأشياء، وإدارتها، وتطبيق الرقع (التصحيحات) عليها، وهو يوصي بكيفية تمكُّن الحكومة الأمريكيّة من أفضل تطبيقٍ لهذه الممارسات (غودلو [Goodloe] ونانْدَراج جالو [Nandaraj Gallo]، 2019). وقد يفرض هذا القانون، الذي يلي تشريعاً سابقاً فاشلاً، معايير محدَّدة من حيث الأمن الإلكتروني لأجهزة إنترنت الأشياء التي تشتريها الوكالات الفيدراليّة أملاً بأن يعتمد المُصنِّعون هذه للسوق التجارية.

ويتمثّل مكوِّنٌ أساسيٌّ في الجهود الرامية إلى تنظيم التكنولوجيات الناشئة بالشراكات بين القطاعيْن العام والخاص. فعلى سبيل المثال، يتعاون المعهد الوطني للمعايير والتكنولوجيا (NIST) مع شركاء من القطاعين العام والخاص لتطوير ممارسات فضلى ومبادئ توجيهية، على غرار إطار عمله للأمن الإلكتروني لإدارة الخطر الإلكتروني. وقد أيّد اتّحاد ابتكار الأجهزة الطبيّة (Medical Device Innovation Consortium [MDIC])، وهو شراكة بين القطاعيْن العام والخاص تشمل الحكومة وأصحاب شأن صناعيين، جهوداً مبذولةً لتعزيز ديناميكية صناعيّة أكثر تعاونيّةً حيث قد يكشف الباحثون عن نقاط ضعْفٍ في هذه الأجهزة الطبيّة بدون خوفٍ من المسؤولية المدنيّة أو الملاحقة الجنائيّة (اتّحاد ابتكار الأجهزة الطبيّة [MDIC]، 2018).[17] وقد وَضَعَت اعتباراً من منتصف عام 2019 أكثر من 20 منظّمة برامج مماثلة (أنا الفارس [آي أم ذا كافالري] [I Am the Cavalry]، غير مؤرَّخ).

وبالإضافة إلى جهود حوكمة الأمن الإلكتروني التي تنطلق من الأعلى نحو القاعدة، سَعَى مؤيّدون متعددون على مستوى الشعب إلى تعزيز الممارسات الفضلى من حيث الأمن الإلكتروني في مجال الأجهزة الطبية المتّصلة. فعلى سبيل المثال، أنتَجَت المنظّمة غير الحكوميّة أنا الفارس (آي أم ذا كافالري) (I Am the Cavalry) ما يُعرف بتسمية "قَسَم أبقراط للأجهزة الطبية المتّصلة" (Hippocratic Oath for Connected Medical Devices)، مع خمسة مبادئ طوعيّة يتوجّب على الجهات المزوِّدَة للرعاية الصحيّة ومُصنِّعي الأجهزة اعتمادها لحماية سلامة المرضى وأمنهم بشكلٍ أفضل (وودز [Woods]، كورافوس [Coravos]، وكورمان [Corman]، 2019). ويرتبط القَسَم بضمان أنّ الأجهزةِ والمعلومات التي تحتويها الأجهزة مرنةٌ في وجه الاختراق، والاعتراض، والتلاعب والكشف غير المصرَّح به، وبأن تكون التحديثات وأعمال الإصلاح الأخرى فورية وفعّالة.

حوكمة بيانات إنترنت الأجسام (IoB)

كما هي الحال بالنسبة إلى أجهزة إنترنت الأجسام (IoB)، ما من كيانٍ واحدٍ يوفّر الرقابة بالنسبة إلى بيانات إنترت الأجسام. ويلخّص الجدول رقم 5 بعض الهيئات الأوّليّة ومسؤولياتها، على الرغم من أنّ اللائحة الإجماليّة لخصوصية المعلومات الشخصيّة مجزّأة على امتداد وكالات حكوميّة وفيدراليّة متعدّدة.[18]

يتمّ تنظيم حماية المعلومات الطبية على المستوى الفيدراليّ، وذلك جزئياً بموجب قانون نقْل التأمين الصحي والمساءلة (HIPAA). ففي غياب قانون فيدرالي آخر يرعى خصوصية البيانات، ينصّ قانون نقْل التأمين الصحي والمساءلة على إطار العمل الرئيسي لحماية البيانات المتعلّقة بإنترنت الأجسام (IoB). بالتحديد، وبموجب قاعدة التبليغ عن الاختراق المنصوص عليها في قانون نقْل التأمين الصحي والمساءلة (HIPAA Breach Notification Rule)، رقم 45 من قانون اللوائح الفيدرالية الفقرات 164.400–414 (45CFR §§ 164.400–414)، تُبَلِّغ الكيانات المشمولة في قانون نقْل التأمين الصحي والمساءلة (أي الجهات المزوِّدَة للخدمات الصحيّة، والخطط الصحية، وغرف مقاصة الرعاية الصحية) الأفراد المتأثرين ما أنّ يتم الوصول إلى معلوماتهم أو الكشف عنها بطريقةٍ غير ملائمة، كما عندما يطّلع موظّف في مستشفى ما على سجلّ مريض، أو عندما يتم فقدان قاعدة بيانات طبيّة أو سرقتها. ويتمثّل جوهر اللائحة بمساءلة المستشفيات والمُمارِسين عن الثغرات في ممارسات أمن البيانات وبإتاحة فرصةٍ للأفراد من أجل رصْد معلوماتهم الماليّة وسجلّاتهم الطبية عن كثب للحؤول دون انتحال الهوية المالية أو الطبية.[19] على الرغم من ذلك، لا يغطّي قانون نقْل التأمين الصحي والمساءلة المعلومات الصحيّة غير الطبية أو البيومترية، وبالفعل إنّه لا يغطي أغلبية البيانات التي تجمعها أجهزة إنترنت الأجسام الاستهلاكيّة.

تساعد لجنة التجارة الفيدراليّة (FTC) في ضمان أمن البيانات وخصوصيّة المُستَهلِكين من خلال دعاوى قضائيّة يرفَعها مكتب حماية المُستَهلِكين (Bureau of Consumer Protection) بموجب القسْم رقم 5 (a) ([Section 5 [a) من قانون لجنة التجارة الفيدراليّة (FTC act)، الذي ينصّ على أنّ "الأفعال أو الممارسات غير العادِلة أو المُضلِّلَة التي تجري في سياق التجارة أو تؤثِّر عليها ... تُعتَبَر غير قانونيّة." (الرقم 15 من مدوّنة القوانين الأمريكيّة القسم رقم 45 [a][1] – [15 U.S.C. Sec. 45[a][1]]). يمكّن هذا لجنة التجارة الفيدراليّة من رفْع دعاوى قضائيّة ضدّ الشركات التي تُبدي نقصاً كبيراً في أمن البيانات أو خصوصيتها، أو التي تكون مُضلِّلَة بشأن طريقة استخدامها للبيانات. وبالنظر إلى دورها الرقابيّ، طوَّرَت لجنة التجارة الفيدراليّة الأداة التفاعليّة للتطبيقات الصحيّة على الهواتف الجوّالة *(Mobile Health Apps Interactive Tool)*، وهي كناية عن قائمة مرجعيّة مُصمَّمَة لمساعَدَة المُطوِّرين على فهْم القوانين التي قد تنطبق على منتجاتهم.

الجدول رقم 5

مسؤوليات حوكمة مُختارَةٌ لبيانات إنترنت الأجسام (IoB)

الوكالة أو المنظّمة	المسؤوليّة
مكتب الحقوق المدنيّة التابع لوزارة الصحة والخدمات البشرية الأمريكية (U.S Department of Health and Human Services Office for Civil Rights)	يقوم بإنفاذ قانون نقْل التأمين الصحي والمساءلة (Health Insurance Portability and Accountability Act [HIPAA])
مكتب المنسّق القومي لتكنولوجيا المعلومات الصحيّة التابع لوزارة الصحة والخدمات البشرية الأمريكية (U.S Department of Health and Human Services Office of the National Coordinator for Health Information Technology)	ينسّق الجهود لضمان قابلية التشغيل المتبادَل للمعلومات الصحيّة، بما فيها السجلات الصحيّة الإلكترونية (EHRs)
لجنة التجارة الفيدراليّة الأمريكية (U.S. Federal Trade Commission [FTC])	تقوم بإنفاذ أمن البيانات وخصوصية المُستَهلِكين من خلال مكتب حماية المُستَهلِكين (Bureau of Consumer Protection)
المدّعي العام في كاليفورنيا (California Attorney General)	يقوم بإنفاذ قانون كاليفورنيا لحماية خصوصية المستهلِك (California Consumer Privacy Act [CCPA])
السلطات الرقابيّة في كل بلد عضو في الاتحاد الأوروبي (European Union [EU])	تقوم بإنفاذ اللائحة التنظيمية العامة لحماية البيانات (GDPR) من أجل حماية المعلومات الشخصيّة لسكّان الاتّحاد الأوروبي

وقد رَفَعَت لجنة التجارة الفيدراليّة دعاوى قضائيّة ضدّ شركات متخصِّصَة في مجال وسائل التواصل الاجتماعيّ وتكنولوجيات أخرى، ولكنّنا لم نجِد سوى أمثلة قليلة حول الدعاوى القضائيّة المرفوعَة من قِبَل لجنة التجارة الفيدراليّة ضدّ مُطوِّري إنترنت الأجسام.[20]

إنّ وسطاء البيانات غير مُنَظَّمين إلى حدٍّ كبير، وإنّما يدعو بعض الخبراء القانونيين لوضْع سياسات لحماية المُستَهلِكين. فقد تمّ تقديم قانون محاسبة وسطاء البيانات وشفافيتهم (Data Broker Accountability and Transparency Act) إلى الكونغرس عام 2017، ولكنّه لم يكتسب زخْماً. وفي يونيو/حزيران 2019، أوصى المُدَّعون العامّون في 43 ولاية بإلقاء نظرةٍ أخرى على توصية لجنة التجارة الفيدرالية الصادرة عام 2014 بأن يؤسس الكونغرس سجلاً فيدرالياً لجميع وسطاء البيانات في البلد (الرابطة الوطنيّة للمُدّعين العامّين [National Association of Attorneys General]، 2019). وقد أصبَحَت فيرمونت الولاية الأولى التي سنَّت قانوناً (الرقم في سجلّ خلفيّة التشريعات العامّة لولاية فيرمونت 764 [القانون رقم 171] – [[Vermont Pub. L. H.764 [Act 171]) ينظِّم وسطاء البيانات، والذي دَخَلَ حيّز التنفيذ في 1 يناير/كانون الثاني 2019. ويشترط القانون تسجُّل وسطاء البيانات في قاعدة بيانات عامّة، وتحديد المعلومات التي لا يستطيع مُستهلكٌ ما الانسحاب منها، وشرْح الخيارات بالنسبة إلى الأمور التي يستطيع المُستَهلِك الانسحاب منها، وذِكْر ما إذا حصَل اختراق للبيانات خلال العام الماضي. واعتباراً من يوليو/تموز 2019، تُعتَبَر فيرمونت الولاية الوحيدة التي سنَّت سياسات تجعل نشاط وسطاء البيانات أكثر شفافيّة.

وبما أنّه ليس للولايات المتّحدة قانونٌ فيدراليٌ يرعى خصوصية البيانات، أدخَلَت الولايات مجموعةً من القوانين واللوائح التي تنطبق على بيانات السكّان الشخصيّة، والتي يشمل بعضها معلوماتٍ مرتبطةً بإنترنت الأجسام. تختلف هذه القوانين اختلافاً كبيراً على امتداد الولايات من حيث أنواع المعلومات المَحْميّة وحقّ الرجوع المُتاح، ولكنّها بالإجمال تسعى إلى حماية سريّة معلومات المُستَهلِكين وإلى ضمان تمكُّن وصول المرضى إلى المعلومات بناءً على الطلب، أو إلى ضمان عدم استخدام المعلومات الصحيّة الشخصيّة أو تبادُلها إلا بناءً على موافَقَة المريض فحسب (سميث [Smith]، 2013).

لكل ولاية أمريكية قانونٌ يشترط أن تقوم الشركات الخاصة والوكالات الحكوميّة بإبلاغ الأفراد لدى الوصول إلى معلوماتهم الشخصيّة أو الكشف عنها بطريقةٍ غير مُصرَّح بها، كما من خلال اختراقٍ للبيانات ("قوانين التبليغ عن الاختراق الأمني" ["Security Breach Notification Laws"]، 2018). وفي حين تختلف شروط التبليغ، والاستثناءات، والعقوبات بعض الشيء، أصبح التبليغ إحدى آليات الإنفاذ الرئيسيّة لفهْم عمليات اختراق البيانات وإدارتها. واعتباراً من 1 يوليو/تموز 2019، سنَّت 16 ولاية قوانين تنصّ صراحةً على شمْل المعلومات البيومترية غير الطبيّة في اللوائح حول اختراق البيانات، على الرغم من أنّ كل ولاية تختلف من حيث تفسيرها للبيانات البيومترية (استناداً إلى هينيسي وآخرين [Hennessy et al.]، 2019). إنّ ويسكونسن هي الولاية الوحيدة التي شَمَلَت الحمض الخلوي الصبغي (الحمض النووي) (DNA) في قانونها بشأن الكشف عن عمليات الاختراق، باعتباره نوعاً محدداً من البيانات المحميّة ومتمايزاً عن المعلومات البيومتريّة (نظام ويسكونسن، الفقرة رقم 134.98 [Wis. Stat. §134.98]).

وقد مرَّرَت إلينوي وتكساس قوانين تُنَظِّم ما إذا باستطاعة الكيانات التقاط المعلومات البيومترية أو جمْعها لأغراض تجاريّة بدون الحصول على موافقة، حاصِرَةً المعلومات البيومترية "بمسحٍ لشبكة العين أو قزحيّة العين، أو بصمة الإصبع، أو بصمة الصوت، أو سجلٍّ لشكل اليدّ أو الوجه" (قانون إلينوي حول خصوصيّة المعلومات البيومترية [Illinois Biometric Infromation Privacy Act]، 2019؛ قانون تكساس للأعمال والتجارة [Texas Business and Commerce Code]، الفصل رقم 11، العنوان الفرعي A، الفصل رقم 503، 2009). كما مرَّرَت واشنطن قانوناً دخل حيّز التنفيذ في 1 مارس/آذار 2020، يشترط على الكيانات الكشف عن جمْع البيانات البيومترية وتخزينها لأغراض تجارية، أو الحصول على الموافقة، أو تطوير إجراءات تُحظِّر بيع تلك المعلومات في وقتٍ لاحق، حيث تشمل البيانات البيومترية "أنماطاً أو خصائص بيولوجيةً فريدة ... مُستَخدَمَة لتحديد فردٍ محدّد" (قانون واشنطن المُنقَّح [Revised Code of Washington]، الفصل رقم 19.375، 2019). واقترَحَت 12 ولاية أخرى على الأقلّ تشريعاتٍ مماثلةً حول خصوصية البيانات البيومترية.

يهدف قانون كاليفورنيا لحماية خصوصية المستهلِك (CCPA)، الذي دخَل حيّز التنفيذ في 1 يناير/كانون الثاني 2020 إلى تحسين خصوصيّة المُستَهلِكين من خلال منْح الأفراد الحقّ في معرفة المعلومات التي يتمّ جمْعها بشأنهم، وأغراض ذلك الجمْع، والمجالات التي سيتمّ تبادل تلك المعلومات فيها. ويستطيع المُستَهلِكون أيضاً الانسحاب من شركة أعمال تبيع بياناتهم الشخصيّة، ويشترط القانون قيام شركات الأعمال التي تجمع معلومات شخصيّة بحذْف السجلّ بناءً على طلب المُستَهلِكين. يتم تقديم تعريف واسع النطاق للبيانات الشخصيّة في قانون كاليفورنيا لحماية خصوصية المستهلِك وهو يشمل المعلومات البيومترية، وبيانات الموقع الجغرافي، وحتّى الاستدلالات من البيانات المُستَخدَمَة لتشكيل ملفٍّ شخصيٍّ نفسيٍّ للشخص. وقد أصدَرَت ثماني ولايات أخرى على الأقلّ مسودّات لقوانين مماثلة بشأن خصوصية البيانات.

أمّا الاتحاد الأوروبي (European Union) فقد سنّ اللائحة التنظيمية العامة لحماية البيانات (GDPR)، وهي مجموعة من اللوائح مُصمَّمَة لحماية المعلومات الشخصيّة لسكّان الاتحاد الأوروبي (EU)، وتنطبق أيضاً على مُطوِّري إنترنت أجسام البرمجيات أو المعدّات الحاسوبيّة ومُصنّعيه. تشترط اللائحة التنظيمية العامة لحماية البيانات أن يعطي المُستَخدِمون الموافقة المستنيرة قبل أن يجري جمْع معلوماتهم الشخصيّة، وأن تتم حماية

معلوماتهم على مستوى يتلاءم مع مستوى الخطر (الضرر) اللاحق بالمُستَخدِم. بالإضافة إلى ذلك، تمنح اللائحة التنظيمية العامة لحماية البيانات مواطني الاتحاد الأوروبي حقوقاً بشأن البيانات التي تجمعها الشركات منهم، بما في ذلك الحقّ في الوصول إلى البيانات، أو حذْفها، أو نقْلها إلى جهات أخرى معنية بمراقبة البيانات. ويعمل المُشرّعون في الكونغرس على لوائح قد تحدّد معياراً أمريكياً لحماية بيانات المُستهلِكين وسُبُل انتصاف شبيهة لتلك التي تنصّ عليها اللائحة التنظيمية العامة لحماية البيانات أو قانون كاليفورنيا لحماية خصوصية المستهلِك، ولكنّهم لم يسنّوا أي سياسات اعتباراً من يونيو/حزيران 2019 (راتنام [Ratnam]، 2019).

يُمَكِّن بشكلٍ محتمل عدم الاتساق في قوانين إنترنت الأجسام فيما بين الولايات وبين الدولة والمستوى الفيدرالي ظهور فجوات تنظيمية وتحديات من حيث الإنفاذ. فكما هي الحال في مجالات متعددة، تجاوَزَت وتيرة التقدّمات السريعة على مستوى تكنولوجيات إنترنت الأجسام تطوير السياسات لمعالَجَة مخاطرها. ستستدعي هذه السياسات التنقّل الدقيق بين حالتيْن قصويين هما نقْص التنظيم الذي يعجز عن التخفيف من المخاطر وفرْط التنظيم الذي يُحْبِط الابتكار المفيد اجتماعياً أو اعتماد المُستهلِكين له. وسيكون تحقيق التوازن بين الابتكار والتنظيم أمراً ملحاً لحماية المُستهلِكين مع الحفاظ على المنافع والإبقاء على موقع الولايات المتحدة الرياديّ في هذا المجال التنافسيّ.

التطلُّع قُدُماً لمعالَجَة الخطر

لقد استَكْشَفَت هذه الدراسة النظام البيئي المُعَقَّد والآخذ بالتقدّم لإنترنت الأجسام (IoB) وحدَّد مجموعة من المنافع والمخاطر المحتَمَلَة. يضطلع أصحاب شأن حكوميون وغير حكوميين متعددون بدورٍ في هذا النظام البيئي، وقد يتّخذ كل صاحب شأن خطوات بنّاءة في سبيل معالَجَة مجالات الخطر. ففي حال عدم معالَجة هذه المخاطر بشكلٍ ملائم، لن يتم تحقيق منافع إنترنت الأجسام الطبية، والصحية، والأخرى تحقيقاً تاماً.

تعزيز الأمن القومي

تجمع أجهزة إنترنت الأجسام (IoB) معلومات شخصيّة حسّاسة يمكن استخدامها من قِبَل خصومٍ أجانبٍ للتجسُّس أو للتدخُّل في قيمٍ وممارساتٍ مهمّةٍ بالنسبة إلى الأمريكيين. للكونغرس والسلطة التنفيذيّة (Executive Branch) أدوار محدّدة للاحتراز من هذه المخاطر. وستدعو الحاجة إلى توسيع نطاق هذه الجهود بما يتجاوز سياسات الأمن القومي التقليديّة للتعامل أيضاً مع الديناميكيات الجديدة المرتبطة باستخدام إنترنت الأجسام المُنتَشر على نطاقٍ واسعٍ ومع التهديدات الناجمَة عن الخصوم.

فلو سارَت أحداث شركة ستراڤا (Strava) ونائب الرئيس تشيني (Vice President Cheney) بشكلٍ مختلف، لكانت التداعيات هائلة. يمكن أن تأخذ الوزارات الحكوميّة هذه الحوادث بمثابة عِبَرٍ مُستَخلَصَة حول المخاطر التي يتسبب بها إنترنت الأجسام وتطوير استجاباتٍ ملائمة، كما فعلَت وزارة الدفاع الأمريكية (Department of Defense). فعلى سبيل المثال، يمكن تطوير مبادئ توجيهيّة حول استخدام إنترنت الأجسام للمسؤولين الحكوميين ذوي المراتب العالية.

ومع انتشار استخدام إنترنت الأجسام في الأنظمة الاستبداديّة، يمكن أن تُدْرِج وزارة التجارة الأمريكيّة (U.S. Commerce Department) شركات إنترنت الأجسام الأجنبيّة على "لائحة الكيانات" ("Entity List") الخاصة بها، لمنْعها من ممارسة الأعمال مع الأمريكيين، وذلك في حال كانت تلك الشركات الأجنبية متورّطةً في انتهاكاتٍ لحقوق الإنسان. وقد تم تطبيق ذلك بحقّ كيانات صينيّة تقمع الأيغور (Uighur) ومجموعات أخرى من الأقليّات (موس [Moss]، 2019). كما يجب أن تواصل أيضاً لجنة الاستثمار الأجنبي في الولايات المتحدة (CFIUS) رصْد الاستثمار الأجنبي في الشركات الأمريكيّة وشرائها والتحقيق فيهما، ولا سيما تلك التي تعالج بيانات إنترنت الأجسام الحسّاسة والخاصة بالأمريكيين.

قد تزيد التهديدات التي تطال شبكات الاتصالات الأمريكية مع اكتساب إنترنت الأجسام الشعبية، ولذلك، مع نشْر معايير شبكة الجيل الخامس (5G)، والجيل السادس من شبكة تقنية الاتصال اللاسلكي 6 (الواي فاي 6) (Wi-Fi 6)، وإنترنت الأقمار الاصطناعية، يجب أن تموّل الحكومة الفيدراليّة بشكلٍ استباقيٍّ الدراسات وتعمل مع الخبراء لتطوير لوائح بشأن الأمن.

الدفْع بالأمن الإلكتروني قُدُماً

تقترن التكنولوجيات المتّصلة بالشبكة جميعها بخطر من حيث الأمن الإلكتروني، ولكن تثير حساسيّة معلومات إنترنت الأجسام (IoB) والتأثيرات الطبية والصحية المحتملة الناتجة عن تعطيل إنترنت الأشياء أو التلاعب به قلقاً كبيراً. وبحسب ما تمّ وصْفه سابقاً، سعى أصحاب الشأن إلى تعزيز الممارسات الفضلى المتعلقة بالأمن الإلكتروني لأجزاءٍ من النظام البيئي لإنترنت الأجسام، بما في ذلك من خلال جهودٍ تمّ بذلْها بقيادة إدارة الغذاء والدواء (FDA)، ووزارة الأمن الداخلي في الولايات المتحدة (U.S. Department of Homeland Security)، ووزارة التجارة الأمريكيّة (Department of Commerce)، ومنظّمات غير حكومية. على الرغم من ذلك، لا تخضع أجهزة إنترنت الأجسام جميعها لرقابة إدارة الغذاء والدواء، ولم تضع الحكومة الفيدراليّة معايير مُلزِمةً من حيث الأمن الإلكتروني لإنترنت الأجسام. وثمّة فرص للقيام بالمزيد من أجل تعزيز الأمن الإلكتروني لإنترنت الأجسام.

قد تنظر أولاً الحكومة الفيدراليّة، بما فيها الوكالات التنفيذيّة والكونغرس، في كيفية تطبيق مقاربةٍ لإدارة المخاطر تحدّد الممارسات الفضلى والمعايير من حيث الأمن الإلكتروني لمجموعة منتجات إنترنت الأجسام الكاملة. فعلى سبيل المثال، يمكن تصميم إطار

عمل محدّد لإنترنت الأجسام على شَكْل إطار عمل الأمن الإلكتروني الصادر عن المعهد الوطني للمعايير والتكنولوجيا (NIST). سيكون هذا الجهد أكثر فعاليّةً في حال تم بذْله بالتشاور مع منظّمات صناعيّة وممارسين طبيين لضمان فهْم الحكومة للتكنولوجيا والتكاليف المصاحِبة للاقتراحات المتعلّقة بالأمن القومي، بما فيها العوائق في وجه الابتكار، فهماً كاملاً. والأمر المهمّ هو أنّ مقاربةً تنظر في المجموعة الكاملة لأجهزة إنترنت الأجسام قد تتجاوز الجهود القائمة التي تبْذلها إدارة الغذاء والدواء لتشمل أيضاً الأجهزة الصحية الاستهلاكية والسجلات الصحيّة الإلكترونية (EHRs). وفي سياق مقاربة إدارة المخاطر هذه، سيكون من المهم النظر في كيفية تحفيز الاستبعاد الأسرع للأجهزة الطبية القديمة التي تقترن بأمن إلكتروني ضعيف والتي تُستخدم أصلاً على نطاقٍ واسع. فقد تتمثّل خطوة ممكنة بتطوير شهاداتٍ للأمن الإلكتروني لإنترنت الأجسام وإدارتها (بما يشبه ملصق نجمة الطاقة [Energy Star] أو ملصق القيمة الغذائية) والتي، بدلاً من فرْض معيارٍ أدنى معيّنٍ للأمن الإلكتروني، قد تمنح المُستَهلِكين توعية أكبر بشأن أمن المنتجات الإلكتروني وتُمَكِّن بالتالي حوافز السوق لمُصنّعي أجهزة إنترنت الأجسام لاتّباع المبادئ التوجيهية المحددة للأمن الإلكتروني ("كيف يحصل منتجٌ ما على ملصق نجمة الطاقة" "How a Product Earns the ENERGY STAR Label"]، غير مؤرَّخ). يجب دراسة هذا الاقتراح، بالإضافة إلى اقتراحات أخرى، بالتعاون مع أصحاب الشأن.

بالإضافة إلى الجهات الفاعِلة الحكوميّة، تدعو الحاجة إلى نَظَر الجهات المُزوِّدَة للرعاية الصحيّة في التداعيات من حيث الأمن الإلكتروني لدى التوصية بإنترنت الأجسام أو استخدامه. وكخطوةٍ أولى، يجب أن تواصل الأوساط الطبيّة الاستفادة من الخبرة في مجال الأمن الإلكتروني، وذلك مثلاً من خلال استخدام المبادئ التوجيهية المنشورة التي تقدّم المشورة حول كيفية بناء قوى عامِلَة إلكترونيّة مُتَخَصِّصَة في الرعاية الصحيّة.[21] وقد تتعهّد الجهات المزوِّدَة أيضاً بدعْم قَسَم أبقراط للأجهزة الطبية المتّصلة (Hippocratic Oath for Connected Medical Devices)، الذي وضَعَته منظّمة أنا الفارس (آي أم ذا كافالري) (I Am the Cavalry) القائمة على مستوى الشعب، والتي تُشجِّع الجهات المزوِّدَة للرعاية الصحيّة وأصحاب الشأن على الإقرار بأهميّة الأمن الإلكتروني بالنسبة إلى المرضى.

بالمثل، يجب أن يكون مُطوِّرو إنترنت الأجسام أكثر تنبُّهاً إلى الأمن الإلكتروني، وذلك مثلاً من خلال اتّباع المبادئ التوجيهية المتعلّقة بالأمن الإلكتروني الصادرة عن إدارة الغذاء والدواء (حتّى وإنْ لم يكن الجهاز جهازاً طبياً) ومن خلال دمْج اعتبارات الأمن الإلكتروني والخصوصيّة منذ بداية تطوير المنتجات. يجب أن يختبر مُصَنِّعو الأجهزة البرمجيات لتحديد نقاط الضعف بشكلٍ متكرر، بما في ذلك من خلال استخدام برامج الكشف عن نقاط الضعف، وابتكار أساليب ليقوم المُستَخدِمون بتطبيق الرقع (التصحيحات) على البرمجيات. بالإضافة إلى ذلك، يجب أن يضع مُصَنِّعو الأجهزة سياسات لتبليغ المُستهلِك وحمايته في حال بروز قضايا متعلقة بالأمن الإلكتروني أو أخرى (مثلاً، إذا دَعَت الحاجة إلى تطبيق الرقع [التصحيحات] على الجهاز وإلا يتوقّف دعْمه من قِبَل المُصَنِّع). وسيتوجَّب أن ينظر هذا الجهد في تحدّيات الأمن الإلكتروني الفريدة بالنسبة إلى إنترنت الأجسام ومعالجتها، مثل تحدّي تطبيق الرقع (التصحيحات) على الأجهزة التي تمّ زرْعها في الجسم ولا يمكن سحْبها بسهولة. وتشمل ممارسات فضلى أخرى في مجال الأمن الإلكتروني بالنسبة إلى إنترنت الأجسام نمذجة التهديد، ومعايير تخزين البيانات، والاحتفاظ بمستودعٍ لرمز مصدر البرمجيات والذي يمكن أن يراجعه باحثون مستقلّون في مجال الأمن الإلكتروني.

ضمان الخصوصيّة

ليس لدى الولايات المتّحدة قانون فيدراليّ شامل يرعى خصوصيّة البيانات، وإنّ جزءاً كبيراً من البيانات التي يجمعها إنترنت الأجسام (IoB) غير مُنَظَّم بموجب قانون الدولة القائم. إنّها مجالات معقّدة من السياسات، ويُعتبر نطاق إنترنت الأجسام واسعاً، لذلك فإنّه من غير المُرجَّح أن تتمكّن سياسةٌ واحدةٌ من معالجتها جميعها. فلمعالجة المخاطر التي تهدّد الخصوصيّة والناتجة عن أجهزة إنترنت الأجسام، يجب أن ينظر الكونغرس في وضْع معايير فيدراليّة لشفافية البيانات وحمايتها بالنسبة إلى البيانات التي يتم جمْعها من هذه الأجهزة. وفي ظل الظروف الحالية، يتمتّع المُستهلِكون بقدرة محدودة على تحديد الجهة التي تخزِّن بياناتهم الصحيّة والأخرى الحميمة وكيفية استخدام تلك البيانات، ولذلك، وبمثابة نقطة انطلاق للتنظيم، يمكن أن تتخذ الكيانات الحكومية خطوات لضمان شفافية أكبر حول ممارسات جمْع البيانات. ومع نشوء التداعيات الناتجة عن لوائح مثل اللائحة التنظيمية العامة لحماية البيانات (GDPR) وقانون كاليفورنيا لحماية خصوصية المستهلِك (CCPA)، يمكن أن يستنتج الكونغرس عبَراً من نجاحاتها وإخفاقاتها على حدٍّ سواء للنظر في كيفية منْح مُستَخدِمي إنترنت الأجسام حقوقاً بشأن معلوماتهم الشخصيّة، بما في ذلك الحقّ في الانسحاب من عملية الجمْع. وقد تنظر الحكومة الفيدرالية وحكومات الولايات أيضاً في اللوائح المتعلقة بوسطاء البيانات، والقيود المفروضة على الجهات التي يمكنها جمْع البيانات، وكيفية استخدام هذه المعلومات، وما إذا يتمّ بيعها إلى أطراف ثالثة، وما إلى هنالك.

ثمّة أيضاً دورٌ يجب أن تضطلع به الحكومة الفيدرالية لتوحيد مجموعة قوانين الولايات بخصوص عمليات اختراق البيانات والمعلومات الصحيّة من خلال معيارٍ فيدراليٍّ للتبليغ عن عمليات اختراق البيانات. يمكن أن تشجّع الحكومة الفيدراليّة البحث المستقلّ حول مسائل ناشئة مثْل تحمُّل البيانات، والخصوصية بعْد الوفاة، والحق في النسيان فيما يتعلّق ببيانات إنترنت الأجسام، وأن تموّلها. وتدعو الحاجة أيضاً إلى وضْع قواعد لكيفيّة السماح لشركات التأمين، أو أصحاب العمل، أو آخرين باستخدام بيانات إنترنت الأجسام.

يتمّ تشارُك الصلاحيات والموارد المتعلقة بالخصوصية في

مجال البيانات الصحية وبيانات إنترنت الأجسام بين مجموعة من المنظّمات الحكومية، بما فيها لجنة التجارة الفيدراليّة (FTC)، والمعهد الوطني للمعايير والتكنولوجيا (NIST)، ووزارة الصحة والخدمات البشرية الأمريكيّة (Health and Human Services) (والتي تُعتَبَر إدارة الغذاء والدواء [FDA] جزءاً منها). ويتوجّب على الكونغرس اتّخاذ قرارٍ بشأن المجموعة الفرعيّة الأكثر ملاءمةً من بين هذه المنظّمات لإنفاذ السياسات التي ترعى حالات انتهاك الخصوصيّة وحماية البيانات بخصوص أجهزة إنترنت الأجسام. وقد تدعو الحاجة إلى تخصيص موارد إضافيّة ليتوفّر الدعم الكافي لإنفاذ اللوائح في الوقت الذي تصبح فيه منتجات إنترنت الأجسام أكثر انتشاراً على نطاقٍ واسع. فعلى سبيل المثال، للجنة التجارة الفيدرالية في ظل الظروف الحالية 40 موظّفاً فقط يعملون بدوامٍ كاملٍ ومخصصين لخصوصيّة البيانات (بالمقارنة مع 500 موظّف في سلطة حماية البيانات في المملكة المتحدة)، وقد ذَكَر رئيس لجنة التجارة الفيدرالية جوزيف سايمونز (FTC Chairman Joseph Simons) أنّ الوكالة لا تملك موارد كافية لزيادة مستوى إنفاذها لقوانين خصوصية البيانات (سايمونز [Simons]، 2019).

نشْر التوعية

لقد أدّى التقدُّم السريع لإنترنت الأجسام (IoB) إلى قيام بيئةٍ حيث قد يَسْتَخْدِم المُستهلِكون عن غير قصد إنترنت الأجسام وحيث يسود ارتباك ونقص للوضوح بشأن منافعه وتداعياته الأخلاقيّة السلبيّة المُحْتَمَلَة. قد لا يكون النظام البيئي لإنترنت الأجسام مفيداً بالنسبة إلى الجهات المُزوِّدَة للخدمات الطبيّة أو المُتسهلِكين بقدر ما قد يبدو عليه، أقلّه على المدى القصير. فعلى سبيل المثال، بيّنَ بعض الدراسات أنّ التتبُّع المستمرّ للنشاط البيومتري من خلال تطبيقاتٍ صحيّة، مثْل تطبيقات تتبُع النوم، قد يزيد من قلق المُستَخدِمين ويؤدي إلى تفاقُم حالات مثل الأرق (insomnia) (بارون وآخرون [Baron et al.]، 2017؛ زريك [Zraick] وميرفوش [Mervosh]، 2019). ولم يطوّر بعد عددٌ من تكنولوجيات إنترنت الأجسام قاعدة أدلة سريريّة حول النتائج الطويلة المدى. فسيتوجّب على أصحاب الشأن البحث عن معلومات بخصوص منافع إنترنت الأجسام الواقعية والنفعيّة (البرغماتيّة) وإصدارها مع زيادة انتشارها على نطاق واسع، وأيضاً بخصوص المجالات التي من المرجَّح أن تنشأ الأضرار فيها.

تؤدّي لجنة التجارة الفيدرالية (FTC) أصلاً دوراً مهمّاً في تسويق تكنولوجيات إنترنت الأجسام،[22] وتُتاح للجنة التجارة الفيدراليّة فرصٌ لتأدية دور أكبر من أجل ضمان دعْم ادّعاءات التسويق بشأن تحسين الرفاهية أو علاج صحيّ محدد بالأدلة الملائمة. على الرغم من ذلك، قد تحتاج لجة التجارة الفيدرالية إلى موارد إضافيّة للتعامل مع المجموعة الواسعة لتكنولوجيات إنترنت الأجسام التي اجتاحَت السوق في الأعوام الأخيرة، وسيكون من المهمّ توفير موظّفين إضافيين يتمتعون بالخبرة في مجال إنترنت الأجسام لضمان ألا تكون ادّعاءات مُطوِّري إنترنت الأجسام مُضلِّلَة أو غير عادِلَة.

ثمّة أيضاً فرص لزيادة التوعية بشأن تداعيات إنترنت الأجسام الأخلاقيّة، وذلك مثلاً من خلال تمويلٍ فيدراليٍّ أو من قِبَل المؤسسات للأبحاث المتعلقة بالتباينات المرتبطة بجمْع بيانات إنترنت الأجسام والرعاية الصحية. ويمكن أن يركِّز هذا البحث أيضاً على مدى تعدّي إنترنت الأجسام على الاستقلالية الذاتية في مكان العمل أو بخلاف ذلك تقويض التوقعات المعقولة بشأن الاستقلالية الذاتية أو الخصوصية.

ويمكن أن تعمل أيضاً الحكومة الفيدرالية وحكومات الولايات مع شركاء لتطوير مبادئ توجيهيّة بشأن التطوير والتسويق المسؤولَيْن لإنترنت الأجسام. وقد تتعاون حكومات الولايات مع قادة الفكر في الجامعات ومؤسسات أخرى للاستفادة من الخبرة في مجالات السياسات المرتبطة بإنترنت الأجسام، مثل الأمن الإلكتروني والصحة الرقمية.[23] فقد تساعد هذه الأنواع من الشراكات بين صانعي القرارات والخبراء في تحديد الفجوات في النظام التنظيمي، وتعزيز الابتكار في مجال تطوير التكنولوجيا، وحماية أصحاب الشأن جميعهم.

وحتى في غياب وظيفة الإرغام التنظيمي، يمكن أن يكون مُطَوِّرو إنترنت الأجسام أكثر وضوحاً مع المُستَهلِكين بشأن مخاطر الأمن الإلكتروني والممارسات المتعلّقة بخصوصية البيانات والمرتبطة بمنتجاتهم. يجمع مُطَوِّرو إنترنت الأجسام كميات شاسعة من البيانات الحميمة، ويتوجّب عليهم أن يذكروا بوضوح سياسات الولاية التي ترعى الخصوصية والحصول على الموافقة المستنيرة لممارستهم المُعتَمَدة في جَمْعِها. كما يجب أن تشرح هذه السياسات بشكل مباشرٍ كيف ستتم حماية البيانات، وكيف سيتمّ استخدام هذه البيانات، والجهات التي قد يتمّ تبادُلها معها. ويجب أيضاً أن يثقّف المُطَوِّرون الجمهور العام حول المخاطر المرتبطة بمنتجات إنترنت الأجسام.

وأخيراً، يتوجّب على المرضى والمُسْتَهلِكين الإقرار بمخاطر إنترنت الأجسام والنظر في هذه المخاطر لدى اتخاذ قرار بشأن استخدام هذه الأجهزة. ففي غياب لوائح جديدة، يجب أن يتوخّى المُستَهْلِكون الحذر ويباشروا انطلاقاً من افتراض أنّه ما أن يجمع جهاز إنترنت الأجسام البيانات، لن يتسنّى للمُستَهلِك على الأرجح التحكُّم الكامل بكيفية تخزين تلك البيانات واستخدامها ويجب أن يكون مستعدّاً لاحتمال اختراقها أو تبادُلها بخلاف ذلك على نطاق واسع. وفي نهاية المطاف، يجب أن يكون المُسْتَهْلِكون على وعي بأنّه يتم جَمْع بياناتهم الحميمة من قِبَل كياناتٍ قد لا تأخذ بالضرورة مصالح المُسْتَهْلِكين الفضلى في الاعتبار. فإنّ زيادة التوعية حول النظام البيئي لإنترنت الأجسام ومخاطره أمرٌ أساسيّ.

الملاحظات

[1] بحسب تعريفٍ قدَّمَته ماتويشين (Matwyshyn) لإنترنت الأجسام (IoB)، إنّه "الاعتماد الزاحِف للأجسام البشريّة على البرمجيات، والمعدات الحاسوبية، والإنترنت فيما يتعلّق بنواحٍ رئيسيّةٍ من وظيفتها" (إنترنت الأجسام [The Internet of Bodies]، 2018). ويتم تعريفُ ثلاثةِ أجيالٍ من إنترنت الأجسام هي: خارج الجسم (body-external)، وداخل الجسم (body-internal)، ومدموج مع الجسم (body-melded) (ماتويشين [Matwyshyn]، 2019).

[2] إنّنا نحصر تعريفنا لأجهزة إنترنت الأجسام (IoB) بالتكنولوجيات التي يمكن ربْطها بفردٍ ما بدلاً من التكنولوجيات التي يتم ربْطها بسمات عموميّةٍ إلى حدٍّ ما تخصّ مجمل البشر أو مرضاً معيّناً. بالتالي، لا تُعتبَر قواعد بيانات التسلسلات الجينيّة الكبيرة (مثل قاعدة بيانات التسلسلات جينبنك [GenBank]) من بيانات إنترنت الأجسام، ولا تُعتبر التقنيات (مثل تقنيّات التكرارات العنقودية المتناظرة القصيرة منتظمة التباعد كريسبر [CRISPR]) المُمَكِّنَة من قواعد البيانات هذه من تكنولوجيات إنترنت الأجسام.

[3] تُعرِّف إدارة الغذاء والدواء (FDA) جهازاً طبياً على الشكل التالي (إدارة الغذاء والدواء [FDA]، 2018a):

- أداة، أو جهاز، أو قِطعة، أو آلة، أو تجهيز، أو جهازٌ مزروعٌ في الجسم، أو كاشِف أنبوبي، أو صنف آخر مماثل أو ذو صلة، بما في ذلك مكوِّن جزئي أو أكسسوار والذي يكون: مُحدَّداً في كُتيّب الوصفات الوطني (National Formulary) الرسمي، أو دستور الأدوية الأمريكي (United States Pharmacopoeia)، أو أي ملحق مُرفَق بهما،
- مُصمَّم للاستخدام في سياق تشخيص مرضٍ أو حالات أخرى، أو في العلاج الشافي من المرض، أو التخفيف منه، أو معالجته، أو الوقاية منه، إنْ لدى الإنسان أو الحيوانات الأخرى، أو
- مُصمَّم للتأثير على تركيبة جسم الإنسان أو الحيوانات الأخرى أو على أي واحدة من وظائفه، والذي لا يُحقِّق أغراضه الأوّلية المرجوّة من خلال تفاعلٍ كيميائيٍّ داخل جسم الإنسان أو الحيوانات الأخرى أو عليه والذي لا يعتمد على تأييضه لتحقيق أيٍّ من أغراضه الأوّليّة المرجّوَة.

[4] يتمثّل مفهومٌ متّصلٌ بإنترنت الأشياء (IoT) وإنترنت الأجسام (IoB) بالأنظمة الإلكترونية-الجسديّة. فبحسب برنامج البحث والتطوير في مجال إقامة الشبكات وتكنولوجيا المعلومات Networking and Information Technology Research and Development) [NITRD]) إنّ الأنظمة الإلكترونية-الجسديّة هي "أنظمة ذكيّة متّصلة بالشبكة مع أجهزة استشعار مُضمَّنَة، ومعالِجات، ومُشغِّلات والتي تكون مُصمَّمَة لاستشعار العالَم الماديّ والتفاعل معه (بما في ذلك المُستَخدِمين البشريين)" (برنامج البحث والتطوير في مجال إقامة الشبكات وتكنولوجيا المعلومات [NITRD]، 2015).

[5] ثمّة مصطلحات إضافيّة متعدّدة لم يتمّ وصْفها هنا وتتّصل بإنترنت الأجسام (IoB)، على غرار تكنولوجيّات التعزيز البشري (human enhancement technologies)، وعلْم الأحياء (البيولوجيا) المُصمَّم للهواة (do-it-yourself biology [DIY bio])، والتكنولوجيا الحاسوبيّة التي تربط الدماغ البشريّ بأنظمة اصطناعيّة (wetware) (أي الاتصالات المباشرة بين الدماغ والحاسوب)، وقياس الذات الكمّي (quantified self)، والتي تُشكِّل جزءاً من مجال التكنولوجيات المتّصلة بالجسم هذا الآخذ بالنمو.

[6] إنّنا نُعرِّف الأجهزة القائمة بذاتها *(freestanding devices)* على أنّها تلك التي تقوم وتعمل من تلقاء نفسها، بدون اتّصال مستمرّ بالجسم.

[7] إنّ معيار شبكة تقنية الاتصال اللاسلكي 6 (الواي فاي 6) (Wi-Fi 6)، والذي يُشار إليه أيضاً بتسمية 802.11ax، هو قيد التطوير ويُتَوَقَّع أن يحصل على الموافقة النهائيّة في يونيو/حزيران 2020 ("الجداول الزمنيّة الرسميّة لمشروع مجموعة العمل رقم 802.11 التابِعة لمعهد المهندسين الكهربائيين والإلكترونيين" "Official IEEE 802.11 Working Group Project Timelines"]، 2019).

[8] إنّ سطح هجومٍ ما هو مجموعة نقاط الدخول المُحتَمَلَة جميعها التي يمكن استخدامها لتنفيذ هجومٍ على نظامٍ ما (ماناداتا [Manadhata] ووينج [Wing]، 2010).

[9] على الرغم من ذلك، تعود بالزمن المخاطر التي تهدد السلامة والناجمة عن الأجهزة الطبيّة التي يتمّ التحكُّم بها انطلاقاً من الحواسيب (computer-controlled medical devices) أقلّه إلى عام 1985 (ليفِسون [Leveson]، 1995).

[10] هذه الوثيقة ليست متوفِّرة للجمهور العام.

[11] إنّ هذا هو على الأرجح نقْص في تقدير العدد الفعلي لنقاط الضعف المعروفة، لأنّ هذه القائمة لا تُحدِّد على الأرجح جميع نقاط الضعف الناجمة عن مكتبات البرمجيات المُصمَّمَة لمنتجات أخرى وإنّما المُستَخدَمَة في هذه الأنظمة.

[12] إنّ بيانات عام 2019 غير مشمولة.

[13] يُشكّل الحق في النسيان (right to be forgotten) جزءاً من اللائحة التنظيمية العامة لحماية البيانات (General Data Protection Regulation [GDPR]) الخاصة بالاتّحاد الأوروبي، وإنّما أصبح بالإمكان إنفاذها اعتباراً من يونيو/حزيران 2019 داخل الاتحاد الأوروبي فحسب.

[14] ينطبق حالياً الحقّ القانوني في الخصوصيّة على الأشخاص الذين هم على قيد الحياة وليس على الأشخاص المتوفين (بانتا [Banta]، 2016). وتبقى قواعد الخصوصيّة المنصوص عليها في قانون نقْل التأمين الصحي والمساءلة (HIPAA) ساريةً لمدة 50 عاماً من تاريخ وفاة الشخص المتوفي (وزارة الصحة والخدمات البشرية الأمريكية U.S. Department of Health and Human Services]، 2013).

[15] بحسب ما جادَلَت دراسةٌ حول أخلاقيات التعزيز البشري، "يؤدّي استيعاب أدوات في أشخاصنا إلى اتّصال حميم أو مُعزِّز مع أدواتنا" (ألهوف وآخرون [Allhoff et al.]، 2010).

[16] ثمّة منظّمات أخرى متعدّدة لها مصالح في السلامة الإجماليّة لأجهزة إنترنت الأجسام (IoB) وإنترنت الأشياء (IoT)، على غرار لجنة سلامة المنتجات الاستهلاكية (Consumer Product Safety Commission)، ولكن يخرج إجراء مناقشةٍ كاملةٍ لجميع الهيئات ذات الصلة عن نطاق هذا العمل.

[17] يُعدّ الكشف الآمن عن نقاط ضعْف البرمجيات ترفاً لم يتمتّع بها الباحثون دائماً. ولحسن الحظ، ثمّة حركة متنامية لتغذية عمليةٍ مفتوحةٍ وشفافةٍ لتبليغ البائعين من قِبَل الباحثين.

[18] يخرج إجراء مناقشةٍ كاملةٍ للائحة التي ترعى الخصوصيّة عن نطاق هذا العمل؛ على الرغم من ذلك، راجِع موليغان (Mulligan)، فريمان (Freeman)، ولينبو (Linebaugh) (2019).

[19] على الرغم من ذلك، ليس من المُثبَت ما إذا حسَّنَت هذه القاعدة الممارسات المتعلّقة بأمن البيانات.

[20] يتم وصْف أحد الأمثلة في موريس (Morris) (2017).

[21] إنّ أحد الأمثلة هو "دليل القوى العاملة المعنيّة بالأمن الإلكتروني لقطاع الرعاية الصحيّة" ("Healthcare Industry Cybersecurity Workforce Guide") (مجلس تنسيق قطاعَي الرعاية الصحيّة والصحة العامة Healthcare and Public Health Sector] Coordinating Council]، غير مؤرَّخ). ويكمن مثلٌ آخر، ليس خاصاً بمنظّمات الرعاية الصحيّة بشكلٍ محدد، بـ"إطار عمل القوى العاملة المعنية بالأمن الإلكتروني للمبادرة الوطنيّة للتثقيف حول الأمن الإلكتروني" National Initiative for Cybersecurity) (Education [NICE] Cybersecurity Workforce Framework التابع للمعهد الوطني للمعايير والتكنولوجيا (NIST)، (نيوهاوس وآخرون [Newhouse et al.]، 2017).

[22] ليست لجنة التجارة الفيدراليّة (FTC) المنظّمة الوحيدة المعْنيّة هنا؛ تنظّم إدارة الغذاء والدواء (FDA) مثلاً تسويق الأجهزة الطبية.

[23] فعلى سبيل المثال، عَقَد مركز الحوسبة الجسدية (Center for Body Computing) في جامعة كاليفورنيا الجنوبية (University of Southern California) شراكةً مع مكتب حاكِم كاليفورنيا لتنمية الأعمال والاقتصاد California Governor's Office of Business) and Economic Development) من أجل تطوير مفاهيم الأمن الإلكتروني في مجال تكنولوجيا معلومات الرعاية الصحيّة وتعميمها) مركز الحوسبة الجسدية في جامعة كاليفورنيا الجنوبية University of Southern California Center for Body] Computing]، 2018).



Agboola, Stephen, Kamal Jethwani, Kholoud Khateeb, Stephanie Moore, and Joseph Kvedar, "Heart Failure Remote Monitoring: Evidence from the Retrospective Evaluation of a Real-World Remote Monitoring Program," *Journal of Medical Internet Research*, Vol. 17, No. 4, 2015, p. e101.

Agniel, Denis, Isaac S. Kohane, and Griffin M. Weber, "Biases in Electronic Health Record Data Due to Processes Within the Healthcare System: Retrospective Observational Study," *BMJ*, Vol. 361, 2018, p. k1479.

Allen, Marshall, "Health Insurers Are Vacuuming up Details About You—and It Could Raise Your Rates," *ProPublica*, July 17, 2018a. As of July 3, 2019:
https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates

———, "You Snooze, You Lose: Insurers Make the Old Adage Literally True," *ProPublica*, November 21, 2018b. As of April 27, 2020:
https://www.propublica.org/article/you-snooze-you-lose-insurers-make-the-old-adage-literally-true

Allen-Graham, Judith, Lauren Mitchell, Natalie Heriot, Roksana Armani, David Langton, Michele Levinson, Alan Young, Julian A. Smith, Tom Kotsimbos, and John W. Wilson, "Electronic Health Records and Online Medical Records: An Asset or a Liability Under Current Conditions?" *Australian Health Review*, Vol. 42, No. 1, 2018, pp. 59–65.

Allhoff, Fritz, Patrick Lin, James Moor, and John Weckert, "Ethics of Human Enhancement: 25 Questions & Answers," *Studies in Ethics, Law, and Technology*, Vol. 4, No. 1, 2010, p. Article-4.

Apple, "ECG App and Irregular Heart Rhythm Notification Available Today on Apple Watch," press release, December 6, 2018.

Appleby, Julie, "A Wake-up Call on Smart Beds and Sleep Apps That Collect Your Data," *Time*, May 29, 2019. As of April 27, 2020:
https://time.com/5592792/a-wake-up-call-on-smart-beds-and-sleep-apps-that-collect-your-data/

Atlantic Council, *Cyber Risk Thursday: Internet of Bodies*, webcast, September 21, 2017. As of April 27, 2020:
https://www.atlanticcouncil.org/unused/webcasts/cyber-risk-thursday-internet-of-bodies/

Axon A. I. and Policing Technology Ethics Board, *First Report of the Axon AI & Policing Technology Ethics Board*, June 2019. As of April 27, 2020:
https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5d13d7e1990c4f00014c0aeb/1561581540954/Axon_Ethics_Board_First_Report.pdf

Baenen, Jeff, "Wisconsin Company Holds 'Chip Party' to Microchip Workers," *Chicago Tribune*, August 2, 2017. As of April 27, 2020:
https://www.chicagotribune.com/business/blue-sky/ct-wisconsin-company-microchips-workers-20170801-story.html

Banta, Natalie M., *Death and Privacy in the Digital Age*, North Carolina Law Review, Vol. 94, No. 3, 2016 p. 927. As of April 27, 2020:
https://scholarship.law.unc.edu/nclr/vol94/iss3/4/

Baron, Kelly Glazer, Sabra Abbott, Nancy Jao, Natalie Manalo, and Rebecca Mullen, "Orthosomnia: Are Some Patients Taking the Quantified Self Too Far?" *Journal of Clinical Sleep Medicine*, Vol. 13, No. 2, 2017, pp. 351–354. As of April 27, 2020:
http://jcsm.aasm.org/viewabstract.aspx?pid=30955

Bauerle Danzman, Sarah, and Geoffrey Gertz, "Why Is the U.S. Forcing a Chinese Company to Sell the Gay Dating App Grindr?" *Washington Post*, April 3, 2019. As of April 27, 2020:
https://www.washingtonpost.com/politics/2019/04/03/why-is-us-is-forcing-chinese-company-sell-gay-dating-app-grindr/?noredirect=on&utm_term=.6ca317886ff3

Beardsley, Tod, "R7-2016-07: Multiple Vulnerabilities in Animas OneTouch Ping Insulin Pump," *Rapid7* blog, 2016. As of April 27, 2020:
https://blog.rapid7.com/2016/10/04/r7-2016-07-multiple-vulnerabilities-in-animas-onetouch-ping-insulin-pump/

Bentley, Daniel, "This Hospital Bed Can Save Lives," *Fortune*, March 20, 2018. As of April 27, 2020:
https://fortune.com/2018/03/20/earlysense-hospital-bed/

Binnendijk, Annika, Robert Timothy Marler, and Elizabeth M. Bartels, *Brain-Computer Interfaces: U.S. Military Applications and Implications, An Initial Assessment*, Santa Monica, Calif.: RAND Corporation, RR-2996-RC, forthcoming.

Boughton, C. K., and R. Hovorka, "Is an Artificial Pancreas (Closed-Loop System) for Type 1 Diabetes Effective?" *Diabetic Medicine*, Vol. 36, No. 3, 2019, pp. 279–286.

Bowcott, Owen, "'Right to Be Forgotten' Could Threaten Global Free Speech, Say NGOs," *The Guardian*, September 9, 2018. As of April 27, 2020:
https://www.theguardian.com/technology/2018/sep/09/right-to-be-forgotten-could-threaten-global-free-speech-say-ngos

Braveman, Paula, Catherine Cubbin, Susan Egerter, Sekai Chideya, Kristen Marchi, Marilyn Metzler, and Samuel Posner, "Socioeconomic Status in Health Research: One Size Does Not Fit All," *Journal of the American Medical Assocation*, Vol. 294, No. 22, 2005, pp. 2879–2888.

Brown, Dalvin, "Hacking Diabetes: People Break into Insulin Pumps as an Alternative to Delayed Innovations," *USA Today*, June 5, 2019. As of April 27, 2020:
https://www.wired.com/2014/12/diabetes-patients-hacking-together-diy-bionic-pancreases/

Bryan-Low, Cassell, Colin Packham, David Lague, Steve Stecklow, and Jack Stubbs, "Hobbling Huawei: Inside the U.S. War on China's Tech Giant," Reuters, May 21, 2019. As of April 27, 2020:
https://www.reuters.com/investigates/special-report/huawei-usa-campaign/

Bushatz, Amy, "Army Issues FitBit Bands in Test Fitness Program," press release, Military.com, October 22, 2013. As of April 27, 2020:
https://www.military.com/daily-news/2013/10/22/army-issues-fitbit-bands-in-test-fitness-program.html

Callahan, Daniel, *Bioethics Briefing Book for Journalists, Policymakers, and Campaigns: Health Care Costs and Medical Technology*, Garrison, N.Y.: The Hastings Center, 2008. As of April 27, 2020:
https://www.thehastingscenter.org/briefingbook/health-care-costs-and-medical-technology/

Caplan, Arthur L., and Phoebe Friesen, "Health Disparities and Clinical Trial Recruitment: Is There a Duty to Tweet?" *PLoS Biology*, Vol. 15, No. 3, 2017, p. e2002040.

Dinh-Le, Catherine, Rachel Chuang, Sara Chokshi, and Devin Mann, "Wearable Health Technology and Electronic Health Record Integration: Scoping Review and Future Directions," *JMIR Mhealth Uhealth*, Vol. 7, No. 9, 2019, p. e12861.

Doffman, Zak, "New Pentagon Laser Identifies High-Risk Individuals by Their Heartbeat," *Forbes*, June 27, 2019. As of April 28, 2020:
https://www.forbes.com/sites/zakdoffman/2019/06/27/u-s-military-laser-can-identify-people-by-their-heartbeats-mit-reports/#6e40b06b2dc6

Dolley, Shawn, "Big Data's Role in Precision Public Health," *Frontiers in Public Health*, Vol. 6, 2018, p. 68.

Donahue, Michelle, "How a Color-Blind Artist Became the World's First Cyborg," *National Geographic*, April 3, 2017. As of April 28, 2020:
https://news.nationalgeographic.com/2017/04/worlds-first-cyborg-human-evolution-science/

Downey, C. L., S. Chapman, R. Randell, J. M. Brown, and D. G. Jayne, "The Impact of Continuous Versus Intermittent Vital Signs Monitoring in Hospitals: A Systematic Review and Narrative Synthesis," *International Journal of Nursing Studies*, Vol. 84, 2018, pp. 19–27.

Edinburgh Law School, *MacCormick Fellow Seminar: Prof Andrea Matwyshyn*, YouTube video, October 23, 2018. As of April 28, 2020:
https://www.youtube.com/watch?v=7Cs0yc9u-VE

Emondi, Al, "Next-Generation Nonsurgical Neurotechnology," Defense Advanced Research Projects Agency, webpage, undated. As of April 28, 2020:
https://www.darpa.mil/program/next-generation-nonsurgical-neurotechnology

Entzeridou, Eleni, Evgenia Markopoulou, and Vasiliki Mollaki, "Public and Physician's Expectations and Ethical Concerns About Electronic Health Record: Benefits Outweigh Risks Except for Information Security," *International Journal of Medical Informatics*, Vol. 110, 2018, pp. 98–107.

Etherington, Darrell, "Elon Musk's Neuralink Looks to Begin Outfitting Human Brains with Faster Input and Output Starting Next Year," *TechCrunch*, July 16, 2019. As of April 28, 2020:
https://techcrunch.com/2019/07/16/elon-musks-neuralink-looks-to-begin-outfitting-human-brains-with-faster-input-and-output-starting-next-year/

Faiola, Anthony, and Richard J. Holden, "Consumer Health Informatics: Empowering Healthy-Living-Seekers Through mHealth," *Progress in Cardiovascular Diseases*, Vol. 59, No. 5, 2017, pp. 479–486.

Fanucci, Luca, Sergio Saponara, Tony Bacchillone, Massimiliano Donati, Pierluigi Barba, Isabel Sanchez-Tato, and Cristina Carmona, "Sensing Devices and Sensor Signal Processing for Remote Monitoring of Vital Signs in CHF Patients," IEEE *Transactions on Instrumentation and Measurement*, Vol. 62, 2013, pp. 553–569.

Farivar, Cyrus, "'Stop the Cyborgs' Launches Public Campaign Against Google Glass," *Ars Technica*, March 22, 2013. As of July 9, 2019:
https://arstechnica.com/tech-policy/2013/03/stop-the-cyborgs-launches-public-campaign-against-google-glass/

FDA—*See* U.S. Food and Drug Administration.

Center for Internet Security, "EI-ISAC Cybersecurity Spotlight—CIA Triad," webpage, undated. As of April 27, 2020:
https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-cia-triad/

Chase, Penny, and Steve Christey Coley, "Rubric for Applying CVSS to Medical Devices," MITRE Corp., January 16, 2019.

Chen, Xing, Babak Assadsangabi, York Hsiang, and Kenichi Takahata, "Enabling Angioplasty-Ready 'Smart' Stents to Detect in-Stent Restenosis and Occlusion," *Advanced Science*, Vol. 5, No. 5, 2018, p. 1700560.

Clymo, Rob, "In-Car AI Could Soon Know If You're Having a Good or Bad Day," *TechRadar*, October 4, 2018. As of April 27, 2020:
https://www.techradar.com/news/in-car-ai-could-soon-know-if-youre-having-a-good-or-bad-day

Coates McCall, Iris, Chloe Lau, Nicole Minielly, and Judy Illes, "Owning Ethical Innovation: Claims About Commercial Wearable Brain Technologies," *Neuron*, Vol. 102, No. 4, May 22, 2019, pp. 728–31.

"Common Vulnerability Scoring System SIG," webpage, FIRST, Cary, N.C., undated. As of April 27, 2020:
https://www.first.org/cvss/

Copp, Tara, "Fitbits and Fitness-Tracking Devices Banned for Deployed Troops," *Military Times*, August 6, 2018. As of April 27, 2020:
https://www.militarytimes.com/news/your-military/2018/08/06/devices-and-apps-that-rely-on-geolocation-restricted-for-deployed-troops/

CPDP Conferences, "CPDP 2018: The Internet of (Vulnerable) Bodies," YouTube video, Computers, Privacy and Data Protection, February 6, 2018. As of April 28, 2020:
https://www.youtube.com/watch?v=10Rlk8uj-lo

Das, Ashok Kumar, Sherali Zeadally, and Mohammad Wazid, "Lightweight Authentication Protocols for Wearable Devices," *Computers & Electrical Engineering*, Vol. 63, 2017, pp. 196–208. As of May 13, 2020:
https://www.sciencedirect.com/science/article/pii/S0045790617305347#bib0009

Day, Matt, "Amazon Is Working on a Device That Can Read Human Emotions," Bloomberg, May 23, 2019. As of April 28, 2020:
https://www.bloomberg.com/news/articles/2019-05-23/amazon-is-working-on-a-wearable-device-that-reads-human-emotions

Defense Intelligence Agency, "Challenges to Security in Space," press release, February 11, 2019. As of April 28, 2020:
https://media.defense.gov/2019/Feb/11/2002088710/-1/-1/1/SPACE-SECURITY-CHALLENGES.PDF

Deichmann, Johannes, Kersten Heineke, Thomas Reinbacher, and Dominik Wee, "Creating a Successful Internet of Things Data Marketplace," McKinsey Digital, October 2016. As of July 3, 2019:
https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/creating-a-successful-internet-of-things-data-marketplace

Derousseau, Ryan, "The Tech That Tracks Your Movements at Work," BBC News, June 14, 2017. As of April 28, 2020:
https://www.bbc.com/worklife/article/20170613-the-tech-that-tracks-your-movements-at-work

Griffin, Patrick, "Edit Thyself: Biohacking in the Age of CRISPR," in *Science in the News*, February 14, 2018. As of April 28, 2020:
http://sitn.hms.harvard.edu/flash/2018/edit-thyself-biohacking-age-crispr/

Groll, Elias, "The Enduring Mystery of Who Hacked Anthem," *Foreign Policy*, May 10, 2019. As of April 28, 2020:
https://foreignpolicy.com/2019/05/10/the-enduring-mystery-of-who-hacked-anthem-hackers-spies-china/

Grush, Loren, "SpaceX is in Communication with All But Three of 60 Starlink Satellites One Month After Launch," *The Verge*, June 28, 2019. As of April 28, 2020:
https://www.theverge.com/2019/6/28/19154142/spacex-starlink-60-satellites-communication-internet-constellation

Gryphon Scientific and Rhodium Group, *China's Biotechnology Development: The Role of US and Other Foreign Engagement*, Washington, D.C.: U.S.-China Economic and Security Review Commission, February 14, 2019. As of April 28, 2020:
https://www.uscc.gov/Research/china%E2%80%99s-biotechnology-development-role-us-and-other-foreign-engagement

Gutierrez, Erie G., Nathan E. Crone, Joon Y. Kang, Yaretson I. Carmenate, and Gregory L. Krauss, "Strategies for Non-EEG Seizure Detection and Timing for Alerting and Interventions with Tonic–Clonic Seizures," *Epilepsia*, Vol. 59, 2018, pp. 36–41.

Hambling, David, "The Pentagon Has a Laser That Can Identify People from a Distance—by Their Heartbeat," *MIT Technology Review*, June 27, 2019. As of April 28, 2020:
https://www.technologyreview.com/s/613891/the-pentagon-has-a-laser-that-can-identify-people-from-a-distanceby-their-heartbeat/

Harper, Sarah, *Ageing Societies: Myths, Challenges and Opportunities*, London: Hodder Education, 2006.

Haskins, Caroline, "Revealed: This Is Palantir's Top-Secret User Manual for Cops," *Motherboard*, July 12, 2019. As of July 15, 2019:
https://www.vice.com/en_us/article/9kx4z8/revealed-this-is-palantirs-top-secret-user-manual-for-cops

Healey, Jason, Neal Pollard, and Beau Woods, "The Healthcare Internet of Things: Risks and Rewards," Atlantic Council, March 2015. As of July 13, 2019:
https://www.atlanticcouncil.org/images/publications/ACUS_Intel_MedicalDevices.pdf

Healthcare and Public Health Sector Coordinating Council, "Healthcare Industry Cybersecurity Workforce Guide: Recruiting and Retaining Skilled Cybersecurity Talent," undated. As of August 30, 2019:
https://healthsectorcouncil.org/wp-content/uploads/2019/06/Healthcare-Industry-Cybersecurity-Workforce-Guide-1.pdf

Hennessy, Jennifer J., Chanley T. Howell, Michael R. Overly, Jennifer L. Rathburn, Steven M. Millendorf, Aaron K, Tantleff, Samuel D. Goldstick, and Thomas E. Chisena, "State Data Breach Notification Laws," webpage, Foley & Lardner LLP, updated January 2019. As of April 28, 2020:
https://www.foley.com/en/insights/publications/2019/01/state-data-breach-notification-laws

Hern, Alex, "Fitness Tracking App Strava Gives Away Location of Secret US Army Bases," *The Guardian*, January 28th, 2018. As of April 28, 2020:
https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

Federal Trade Commission,"Complying with the FTC's Health Breach Notification Rule," webpage, April 2010. As of April 28, 2020:
https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule

———, "Careful Connections: Building Security in the Internet of Things," webpage, January 2015. As of April 28, 2020:
https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf

FTC—*See* Federal Trade Commission.

Garg, Satish K., Stuart A. Weinzimer, William Tamborlane, Bruce A. Buckingham, Bruce W. Bode, Timothy S. Bailey, Ronald L. Brazg, Jacob Illany, Robert H. Slover, Stacey M. Anderson, Richard M. Bergenstal, Benyamin Grosman, Anirban Roy, Toni L. Cordero, John Shin, Scott W. Lee, and Francine R. Kaufman, "Glucose Outcomes with the In-Home Use of a Hybrid Closed-Loop Insulin Delivery System in Adolescents and Adults with Type 1 Diabetes," *Diabetes Technology & Therapeutics*, Vol. 19, No. 3, 2017, pp. 155–163.

Geller, Stacie E., Abby Koch, Beth F. Pellettiere, and Molly Carnes, "Inclusion, Analysis, and Reporting of Sex and Race/Ethnicity in Clinical Trials: Have We Made Progress?" *Journal of Women's Health*, Vol. 20, No. 3, 2011, pp. 315–320.

Geller, Stacie E., Abigail R. Koch, Pamela Roesch, Amarette Filut, Emily Hallgren, and Molly Carnes, "The More Things Change, the More They Stay the Same: A Study to Evaluate Compliance with Inclusion and Assessment of Women and Minorities in Randomized Controlled Trials," *Academic Medicine*, Vol. 93, No. 4, 2018, pp. 630–635.

Gillan, Fraser, "The Transhumanists Who Are 'Upgrading' Their Bodies," BBC News, October 6, 2019. As of November 11, 2019:
https://www.bbc.com/news/uk-scotland-49893869

Giuliano, Karen, Wan-Ting Su, Daniel Degnan, Kristy Fitzgerald, Richard Zink, and Poching DeLaurentis, "Intravenous Smart Pump Drug Library Compliance: A Descriptive Study of 44 Hospitals," *Journal of Patient Safety*, Vol. 14, No. 4, 2018, pp. e76–e82.

Glasgow, Russell E., Bethany M. Kwan, and Daniel D. Matlock, "Realizing the Full Potential of Precision Health: The Need to Include Patient-Reported Health Behavior, Mental Health, Social Determinants, and Patient Preferences Data," *Journal of Clinical and Translational Science*, Vol. 2, No. 3, 2018, pp. 183–185.

Gonzales, Amy, "Is Digital Technology Making Health Inequality Worse?" *Interdisciplinary Association for Population Health Science*, November 20, 2017. As of April 28, 2020:
https://iaphs.org/digital-technology-making-health-inequality-worse/

Goodin, Dan, "Serious Flaws Leave WPA3 Vulnerable to Hacks That Steal Wi-Fi Passwords," *Ars Technica*, April 11, 2019. As of April 28, 2020:
https://arstechnica.com/information-technology/2019/04/serious-flaws-leave-wpa3-vulnerable-to-hacks-that-steal-wi-fi-passwords/

Goodloe, Katharine, and Micha Nandaraj Gallo, "Senate Reintroduces IoT Cybersecurity Improvement Act," *Inside Privacy*, March 12, 2019. As of July 3, 2019:
https://www.insideprivacy.com/internet-of-things/senate-reintroduces-iot-cybersecurity-improvement-act/

Khan, Sieeka, "Electronic Tattoos Can Be Made Through Graphene and Silk," *Science Times*, March 13, 2019. As of April 28, 2020: https://www.sciencetimes.com/articles/18598/20190313/electronic-tattoos-made-through-graphene-silk.htm

Klitzman, Robert, *Am I My Genes?: Confronting Fate and Family Secrets in the Age of Genetic Testing*, Oxford, UK: Oxford University Press, 2012.

Knack, Anna, Advait Deshpande, Stijn Hoorens, and Salil Gunashekar, "Wearable Devices: Implications of Game-Changing Technologies in the Services Sector in Europe," *Eurofound*, 2019. As of April 28, 2020: https://www.rand.org/pubs/external_publications/EP67914.html

Kumar, Shefaili, J. Tran Tran, Wei-Nchih Lee, Ben Bradshaw, Luca Foschini, and Jessie Juusola, "Longitudinal Data from Activity Trackers Show That Those with Greater Inconsistency in Activity Levels are More Likely to Develop More Severe Depression," *Value in Health*, Vol. 21, 2018, p. S191.

Lai, A. M., P. Y. S. Hsueh, Y. K. Choi, and R. R. Austin, "Present and Future Trends in Consumer Health Informatics and Patient-Generated Health Data," *Yearbook of Medical Informatics*, Vol. 26, No. 01, 2017, pp. 152–159.

Larson, Erik, "Chinese Citizen Indicted in Anthem Hack of 80 Million People," Bloomberg News, May 9, 2019. As of April 28, 2020: https://www.bloomberg.com/news/articles/2019-05-09/chinese-national-indicted-by-u-s-grand-jury-over-anthem-hack

Lee, Mary, "The 'Internet of Bodies' is Setting Dangerous Precedents," *Washington Post*, October 15, 2018. As of July 13, 2019: https://www.washingtonpost.com/news/theworldpost/wp/2018/10/15/health-data/?utm_term=.ff1d3a1de516

LeMoyne, Robert, Timothy Mastroianni, Donald Whiting, and Nestor Tomycz, *Wearable and Wireless Systems with Internet Connectivity for Quantification of Parkinson's Disease and Essential Tremor Characteristics*, Vol. 31, Wearable and Wireless Systems for Healthcare II, Singapore: Springer, 2019.

Leveson, Nancy G., *Safeware: System Safety and Computers*, Boston, Mass.: Addison-Wesley, 1995.

Lilley, Kevin, "20,000 Soldiers Tapped for Army Fitness Program's 2nd Trial," *Army Times*, July 27th, 2015. As of April 28, 2020: https://www.armytimes.com/news/your-army/2015/07/27/20000-soldiers-tapped-for-army-fitness-program-s-2nd-trial/

Linder, Courtney, "Why This Software Engineer Implanted a Tesla Valet Key into Her Arm," *Popular Mechanics*, August 14, 2019. As of April 28, 2020: https://www.popularmechanics.com/technology/infrastructure/a28698503/tesla-key-implant/

Lupton, Deborah, "Quantifying the Body: Monitoring and Measuring Health in the Age of Mhealth Technologies," *Critical Public Health*, Vol. 23, No. 4, 2013, pp. 393–403.

———, "Critical Perspectives on Digital Health Technologies," *Sociology Compass*, Vol. 8, No. 12, 2014, pp. 1344–1359.

MacMillan, Douglas, "Data Brokers Are Selling Your Secrets. How States Are Trying to Stop Them," *Washington Post*, June 24, 2019. As of July 3, 2019: https://www.washingtonpost.com/business/2019/06/24/data-brokers-are-getting-rich-by-selling-your-secrets-how-states-are-trying-stop-them/?utm_term=.a46f70fcae28

HHS—*See* U.S. Department of Health and Human Services.

Holley, Peter, "Wearable Technology Started by Tracking Steps. Soon, It May Allow Your Boss to Track Your Performance," *Washington Post*, June 28, 2019. As of July 3, 2019: https://www.washingtonpost.com/technology/2019/06/28/wearable-technology-started-by-tracking-steps-soon-it-may-allow-your-boss-track-your-performance/?utm_term=.c7692bb4b23a

"How a Product Earns the ENERGY STAR Label," webpage, U.S. Department of Environmental Protection, U.S. Department of Energy, undated. As of April 28, 2020: https://www.energystar.gov/products/how-product-earns-energy-star-label

"How Insulin Pumps Work," webpage, Diabetes.co.uk, Diabetes Digital Media, January 15, 2019. As of April 28, 2020: https://www.diabetes.co.uk/insulin/how-insulin-pumps-work.html

Hurley, Dan, "Diabetes Patients Are Hacking Their Way Toward a Bionic Pancreas," *Wired*, December 24, 2014. As of April 28, 2020: https://www.wired.com/2014/12/diabetes-patients-hacking-together-diy-bionic-pancreases/

I Am the Cavalry, "Disclosure Programs," webpage, undated. As of April 28, 2020: https://www.iamthecavalry.org/resources/disclosure-programs/

Illinois General Assembly, Biometric Information Privacy Act, 740 Illinois Compiled Statutes 14/1. As of July 3, 2019: http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

"Imagining a New Interface: Hands-Free Communication Without Saying a Word," webpage, Tech@Facebook, July 30, 2019. As of April 28, 2020: https://tech.fb.com/imagining-a-new-interface-hands-free-communication-without-saying-a-word/

International Data Corporation, "The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast," June 18, 2019. As of April 28, 2020: https://www.idc.com/getdoc.jsp?containerId=prUS45213219

Jackson, James K., "The Committee on Foreign Investment in the United States (CFIUS)," Congressional Research Service, RL33388, October 23, 2019. As of April 28, 2020: https://crsreports.congress.gov/product/pdf/RL/RL33388

Jamoon, Eric, Vaishali Patel, Jennifer King, and Michael Furukawa, "National Perceptions of EHR Adoption: Barriers, Impacts, and Federal Policies," 2012 National Conference on Health Statistics, Washington, D.C., August 6–8, 2012.

Jaramillo, Estrella, "Meet the Women's Health Companies Disrupting the Wearable Space," *Forbes*, May 16, 2019. As of April 28, 2020: https://www.forbes.com/sites/estrellajaramillo/2019/05/16/womens-health-companies-disrupting-the-wearable-space/#4d36fdb228b3

Kastrenakes, Jacob, "Wi-Fi 6: Is It Really That Much Faster?" *The Verge*, February 21, 2019. As of April 28, 2020: https://www.theverge.com/2019/2/21/18232026/wi-fi-6-speed-explained-router-wifi-how-does-work

Mulligan, Stephen P., Wilson C. Freeman, and Chris D. Linebaugh, *Data Protection Law: An Overview*, Washington, D.C.: Congressional Research Service, R45631, March 25, 2019. As of April 28, 2020:
https://crsreports.congress.gov/product/pdf/R/R45631

National Association of Attorneys General, "Federal Trade Commission Hearings on Competition and Consumer Protection in the 21st Century: Public Comments of 43 State Attorneys General," June 11, 2019. As of April 20, 2020:
https://www.washingtonpost.com/context/state-ags-call-for-data-regulations/52f85d7a-c512-4eec-bc50-2ac411e2c593/

National Center for Health Statistics, "Health, United States, 2015: With Special Feature on Racial and Ethnic Health Disparities," 2016.

National Institute of Standards and Technology, "NIST Releases Draft Security Feature Recommendations for IoT Devices," press release, August 1, 2019. As of July 7, 2020:
https://www.nist.gov/news-events/news/2019/08/nist-releases-draft-security-feature-recommendations-iot-devices

National Institute of Standards and Technology Cyber Physical Systems Public Working Group, "Framework for Cyber-Physical Systems, Release 1.0," May 2016. As of April 28, 2020:
https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf

Neal, Meghan, "The Internet of Bodies Is Coming, and You Could Get Hacked," *Motherboard*, March 13, 2014. As of July 3, 2019:
https://www.vice.com/en_us/article/gvyqgm/the-internet-of-bodies-is-coming-and-you-could-get-hacked

Networking and Information Technology Research and Development, "Cyber-Physical System Interagency Working Group (2015) CPS Vision Statement," June 3, 2015. As of November 7, 2019:
https://www.nitrd.gov/nitrdgroups/images/6/6a/Cyber_Physical_Systems_(CPS)_Vision_Statement.pdf

Newhouse, William, Stephanie Keith, Benjamin Scribner, and Greg Witte, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," NIST Special Publication 800-181, August 2017. As of April 28, 2020:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

Ng, Alfred, "Security Flaw Allows for Spying over 5G, Researchers Warn," CNET, February 1, 2019. As of April 28, 2020:
https://www.cnet.com/news/security-flaw-allows-for-spying-over-5g-researchers-find/

NIST—*See* National Institute of Standards and Technology.

NITRD—*See* Networking and Information Technology Research and Development.

Oberhaus, Daniel, "This DIY Implant Lets You Stream Movies from Inside Your Leg," *Wired*, August 30, 2019. As of August 30, 2019:
https://www.wired.com/story/this-diy-implant-lets-you-stream-movies-from-inside-your-leg/

Office of the National Coordinator for Health Information Technology, "What Is an Electronic Health Record (EHR)?" webpage, HealthIT.gov, September 10, 2019. As of April 28, 2020:
https://www.healthit.gov/faq/what-electronic-health-record-ehr

Manadhata, Pratyusa K., and Jeannette M. Wing, "An Attack Surface Metric," *IEEE Transactions on Software Engineering*, Vol. 37, No. 3, 2010, pp. 371–386.

Marmot, Michael, "Social Determinants of Health Inequalities," *The Lancet*, Vol. 365, No. 9464, 2005, pp. 1099–1104.

Marr, Bernard, "How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read," *Forbes*, May 21, 2018. As of August 30, 2019:
https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#2df2278360ba

———, "Artificial Intelligence in Your Toilet. Yes, Really!" *Forbes*, May 20, 2019a. As of April 28, 2020:
https://www.forbes.com/sites/bernardmarr/2019/05/20/artificially-intelligent-toilets-yes-they-are-here/2/#477336615a85

———, "Chinese Social Credit Score: Utopian Big Data Bliss or Black Mirror on Steroids?" *Forbes*, January 21, 2019b. As of April 28, 2020:
https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/

Massachusetts Institute of Technology Media Lab, "Project AttentivU," press release, August 20, 2019. As of August 30, 2019:
https://www.media.mit.edu/projects/attentivu/overview/

Matwyshyn, Andrea M., "The Internet of Bodies," *9th Annual Privacy Law Scholars Conference, Berkeley Center for Law & Technology*, Washington, D.C., June 2, 2016. As of April 28, 2020:
https://www.law.berkeley.edu/research/bclt/past-events/2016-conferences/june-2016-the-9th-annual-privacy-law-scholars-conference/program/

———, "The 'Internet of Bodies' Is Here. Are Courts and Regulators Ready?" *Wall Street Journal*, November 12, 2018. As of April 28, 2020:
https://www.wsj.com/articles/the-internet-of-bodies-is-here-are-courts-and-regulators-ready-1542039566

———, "The Internet of Bodies," *William & Mary Law Review*, Vol. 77, No. 1, 2019. As of April 28, 2020:
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3452891

MDIC—*See* Medical Device Innovation Consortium.

Medical Device Innovation Consortium, *Medical Device Cybersecurity Report: Advancing Coordinated Vulnerability Disclosure*, Minneapolis, Minn., October 1, 2018. As of July 3, 2019:
http://mdic.org/wp-content/uploads/2018/10/MDIC-CybersecurityReport.pdf

Meingast, Marci, Tanya Roosta, and Shankar Sastry, "Security and Privacy Issues with Health Care Information Technology," *Proceedings of the 2006 International Conference of the IEEE Engineering in Medicine and Biology Society*, New York, August 31–September 3, 2006, pp. 5453–5458.

Morris, David, "Exercise App Reaches $1 Million FTC Settlement After Breaking Its Promise to Pay Users for Working Out," *Fortune*, September 23, 2017. As of April 28, 2020:
https://fortune.com/2017/09/23/exercise-app-pact-settlement/

Moss, Sebastian, "US Sanctions Chinese Tech Companies Including Sensetime over Human Rights Abuses," *Data Center Dynamics*, October 8, 2019. As of April 28, 2020:
https://www.datacenterdynamics.com/news/us-sanctions-chinese-tech-companies-including-sensetime-over-human-rights-abuses/

Schneeweiss, Sebastian, and Jerry Avorn, "A Review of Uses of Health Care Utilization Databases for Epidemiologic Research on Therapeutics," *Journal of Clinical Epidemiology*, Vol. 58, No. 4, 2005, pp. 323–337.

Schulte, Fred, and Erika Fry, "Death by 1,000 Clicks: Where Electronic Health Records Went Wrong," *Kaiser Health News*, March 18, 2019a. As of April 28, 2020: https://khn.org/news/death-by-a-thousand-clicks/

———, "FDA Chief Calls for Stricter Scrutiny of Electronic Health Records," *Kaiser Health News*, March 21, 2019b. As of April 28, 2020: https://khn.org/news/fda-chief-calls-for-stricter-scrutiny-of-electronic-health-records/

Scott, Emily, "Wearable Device Can Predict Older Adults' Risk of Falling," Carl R. Woese Institute For Genomic Biology, University of Illinois, July 12, 2018. As of April 28, 2020: https://www.igb.illinois.edu/article/wearable-device-can-predict-older-adults-risk-falling

"Security Breach Notification Laws," database, National Conference of State Legislatures, Washington, D.C., updated September 29, 2018. As of April 28, 2020: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Silver, Mike, "Scientists Develop Tiny Tooth-Mounted Sensors That Can Track What You Eat," *Tufts Now*, March 22, 2018. As of July 9, 2019: https://now.tufts.edu/news-releases/scientists-develop-tiny-tooth-mounted-sensors-can-track-what-you-eat

Simons, Joseph, Office of the Chairman, Federal Trade Commission, "Joseph Simons to the Honorable Frank Pallone, Jr., Washington, D.C.," letter, April 1, 2019. As of April 28, 2020: https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/FTC%20Response%20to%20Pallone-Schakowsky.pdf

Slager, Heidi K., Jamie Jensen, Kristin Kozlowski, Holly Teagle, Lisa R. Park, Allison Bieve, and Megan Mears, "Remote Programming of Cochlear Implants," *Otology & Neurotology*, Vol. 40, No. 3, 2019, p. e260.

Smith, Robert Ellis, "Compilation of State and Federal Privacy Laws 2013 Electronic Edition," webpage, *Privacy Journal*, 2013.

Solon, Olivia, "Amazon Patents Wristband That Tracks Warehouse Workers' Movements," *The Guardian*, January 13, 2018. As of April 28, 2020: https://www.theguardian.com/technology/2018/jan/31/amazon-warehouse-wristband-tracking

Stachel, Joshua R., Ervin Sejdić, Ajay Ogirala, and Marlin Mickle, "The Impact of the Internet of Things on Implanted Medical Devices Including Pacemakers, and ICDs," *2013 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*, Minneapolis, Minn., May 6–9, 2013. As of April 28, 2020: https://ieeexplore.ieee.org/document/6555533

Staedter, Tracy, "Satellite Internet Technology Has Ignited a New Space Race," *Now.*, Northrup Grumman, July 3, 2019. As of April 28, 2020: https://now.northropgrumman.com/satellite-internet-technology-has-ignited-a-new-space-race

Steele, Robert, and Andrew Clarke, "The Internet of Things and Next-Generation Public Health Information Systems," *Communications and Network*, Vol. 5, No. 03, 2013, pp. 4–9.

"Official IEEE 802.11 Working Group Project Timelines," Institute of Electrical and Electronics Engineers, September 25, 2019. As of April 28, 2020: http://www.ieee802.org/11/Reports/802.11_Timelines.htm

Okun, Michael S., "Tips for Choosing a Deep Brain Stimulation Device," *JAMA Neurology*, Vol. 76, No. 7, April 2019, pp. 749–750.

Osoba, Osonde A., and William Welser IV, *An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence*, Santa Monica, Calif.: RAND Corporation, RR-1744-RC, 2017. As of April 28, 2020: https://www.rand.org/pubs/research_reports/RR1744.html

Papola, Davide, Chiara Gastaldon, and Giovanni Ostuzzi, "Can a Digital Medicine System Improve Adherence to Antipsychotic Treatment?" *Epidemiology and Psychiatric Sciences*, Vol. 27, No. 3, 2018, pp. 227–229.

Piwek, Lukasz, David A. Ellis, Sally Andrews, and Adam Joinson, "The Rise of Consumer Health Wearables: Promises and Barriers," *PLoS Medicine*, Vol. 13, No. 2, 2016, p. e1001953.

Plowman, R. Scooter, Timothy Peters-Strickland, and George M. Savage, "Digital Medicines: Clinical Review on the Safety of Tablets with Sensors," *Expert Opinion on Drug Safety*, Vol. 17, No. 9, 2018, pp. 849–852.

Purcell, David, H. Irene Hall, Kyle L. Bernstein, Thomas L. Gift, Eugene McCray, and Jonathan Mermin, "The Importance of Population Denominators for High-Impact Public Health for Marginalized Populations," *JMIR Public Health and Surveillance*, Vol. 2, No. 1, May 17, 2016, p. e26.

Ratnam, Gopal, "Progress on Federal Data Privacy Bill Slows in Both Chambers," *Chicago Tribune*, June 26, 2019. As of July 8, 2019: https://www.chicagotribune.com/sns-tns-bc-congress-data-privacy-20190626-story.html

Revised Code of Washington, Chapter 19.375, Biometric Identifiers. As of July 3, 2019: https://app.leg.wa.gov/RCW/default.aspx?cite=19.375

Ross, Julianne, "Smart Scales Measure a Lot More Than Weight," CNN, January 4, 2019. As of April 28, 2020: https://www.cnn.com/2019/01/04/cnn-underscored/best-smart-scales/index.html

Rupert, Douglas J., Rebecca R. Moultrie, Jennifer Gard Read, Jacqueline B. Amoozegar, Alexandra S. Bornkessel, Amie C. O'Donoghue, and Helen W. Sullivan, "Perceived Healthcare Provider Reactions to Patient and Caregiver Use of Online Health Communities," *Patient Education and Counseling*, Vol. 96, No. 3, 2014, pp. 320–326.

Russo, Massimo, and Michael Albert, "How IoT Data Ecosystems Will Transform B2B Competition," *Boston Consulting Group*, July 27, 2018. As of July 3, 2019: https://www.bcg.com/en-us/publications/2018/how-internet-of-things-iot-data-ecosystems-transform-b2b-competition.aspx

Samuel, Sigal, "How Biohackers Are Trying to Upgrade Their Brains, Their Bodies—and Human Nature," *Vox*, June 25, 2019. As of April 28, 2020: https://www.vox.com/future-perfect/2019/6/25/18682583/biohacking-transhumanism-human-augmentation-genetic-engineering-crispr

Savage, Maddy, "Thousands of Swedes Are Inserting Microchips Under Their Skin," NPR, October 22, 2018. As of April 28, 2020: https://www.npr.org/2018/10/22/658808705/thousands-of-swedes-are-inserting-microchips-under-their-skin

University of Southern California Center for Body Computing, "Cybersecurity in Healthcare: How California Business can Lead," white paper, 2018. As of April 28, 2020:
https://www.uscbodycomputing.org/uncensored/2018/9/24/z6l7c4u7dmu6dqi1e5rvmc7hhujlh6

U.S. Code, Title 15, Section 45, Unfair Methods of Competition Unlawful; Prevention by Commission.

U.S. Consumer Product Safety Commission, "Provata Health Recalls Promotional Activity Trackers Due to Burn Hazard," September 25, 2018. As of April 27, 2020:
https://www.cpsc.gov/Recalls/2018/Provata-Health-Recalls-Promotional-Activity-Trackers-Due-to-Burn-Hazard

U.S. Department of Health and Human Services, "Health Information of Deceased Individuals: 45 CFR 160.103, Paragraph (2)(iv) of the Definition of 'Protected Health Information,'" September 2013. As of April 28, 2020:
https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/health-information-of-deceased-individuals/index.html

U.S. Food and Drug Administration, "Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software," January 14, 2005. As of July 3, 2019:
https://www.fda.gov/media/72154/download

———, "Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff," December 28, 2016. As of April 28, 2020:
https://www.fda.gov/media/95862/download

———, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff," October 18, 2018d. As of July 3, 2019:
https://www.fda.gov/media/86174/download

———, "FDA Approves First Continuous Glucose Monitoring System with a Fully Implantable Glucose Sensor and Compatible Mobile App for Adults with Diabetes," press release, June 25, 2018b. As of April 28, 2020:
https://www.fda.gov/news-events/press-announcements/fda-approves-first-continuous-glucose-monitoring-system-fully-implantable-glucose-sensor-and

———, "Medical Device Overview," webpage, September 14, 2018a. As of April 28, 2020:
https://www.fda.gov/industry/regulated-products/medical-device-overview

———, "Medical Device Recalls," webpage, September 26, 2018c. As of April 28, 2020:
https://www.fda.gov/medical-devices/medical-device-safety/medical-device-recalls

———, "Cybersecurity," webpage, June 27, 2019a. As of July 3, 2019:
https://www.fda.gov/medical-devices/digital-health/cybersecurity

———, "Cybersecurity Vulnerabilities Affecting Medtronic Implantable Cardiac Devices, Programmers, and Home Monitors: FDA Safety Communication," webpage, March 21, 2019b. As of April 28, 2020:
https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-affecting-medtronic-implantable-cardiac-devices-programmers-and-home

Strathspey Crown, "Strathspey Crown LLC Announces Issuance of US Patent of the First Implantable Intraocular Lens (IOL) with a Video Camera and Wireless Transmission Capability," July 12, 2017. As of April 28, 2020:
http://strathspeycrown.com/assets/pdf/1505148854250fc4abc8da4e88d59bf6d0486bf1cc.pdf

Stück, David, Haraldur Tómas, Greg Ver Steeg, Alessandro Epasto, and Luca Foschini, "Novel Digital Voice Biomarkers of Dementia from the Framingham Study," *Alzheimer's & Dementia: The Journal of the Alzheimer's Association*, Vol. 14, No. 7, 2018, pp. 778–779.

Sullivan, Tom, "Why EHR Data Interoperability Is Such a Mess in 3 Charts," *Healthcare IT News*, May 16, 2018. As of April 28, 2020:
https://www.healthcareitnews.com/news/why-ehr-data-interoperability-such-mess-3-charts

Swearingen, Jake, "Europe's 'Right to Be Forgotten' Will Be Staying in Europe," *New York Magazine*, January 10, 2019. As of April 28, 2020:
http://nymag.com/intelligencer/2019/01/europes-right-to-be-forgotten-will-be-staying-in-europe.html

Texas Business and Commerce Code, Title 11, Subtitle A, Chapter 503, Biometric Identifiers. As of April 28, 2020:
https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm

"The Case Against a Right to Be Forgotten," *Law Times*, September 17, 2018. As of April 28, 2020:
https://www.lawtimesnews.com/article/the-case-against-a-right-to-be-forgotten-16216/

The Internet of Bodies, "Chat re: IoB–FTC Comm. @TerrellMcSweeny & @amatwyshyn," Twitter moment, March 7, 2018. As of April 28, 2020:
https://twitter.com/i/moments/1062106824449634304

ThreatConnect Research Team, "The Anthem Hack: All Roads Lead to China," *ThreatConnect* blog, February 27, 2015. As of April 28, 2020:
https://threatconnect.com/blog/the-anthem-hack-all-roads-lead-to-china/

Tibken, Shara, and Robert Cheng, "Hearing Aids Are Getting Smarter. Think AI, Health Tracking," CNET, April 5, 2018. As of July 9, 2019:
https://www.cnet.com/news/hearing-aids-now-theyre-internet-ai-and-health-devices-starkey-oticon-harman-bose/

Trammell, Dustin D., "Differences: Bodyhacking vs Biohacking," in *BodyHackingCon* blog, September 26, 2015. As of April 28, 2020:
https://bodyhackingcon.com/blog/differences-bodyhacking-vs-biohacking.html

Trauth, Erin, and Ella Browning, "Technologized Talk: Wearable Technologies, Patient Agency, and Medical Communication in Healthcare Settings," *International Journal of Sociotechnology and Knowledge Development (IJSKD)*, Vol. 10, No. 3, 2018, pp. 1–26.

Turk, Victoria, "This Sleep-Tracking Ring Can Detect When You've Drunk Too Much," *Wired*, June 18, 2019. As of April 28, 2020:
https://www.wired.co.uk/article/oura-ring-uk-sleep-tracking

United Nations, *World Population Ageing 2015 (ST/ESA/SER.A/390)*, New York: United Nations Department of Economic and Social Affairs Population Division, 2015.

Wootson, Cleve R., "A Man Detailed His Escape from a Burning House. His Pacemaker Told Police a Different Story," *Washington Post*, February 8, 2017. As of July 3, 2019: https://www.washingtonpost.com/news/to-your-health/wp/2017/02/08/a-man-detailed-his-escape-from-a-burning-house-his-pacemaker-told-police-a-different-story/?utm_term=.f0b9a4d2b9dd

World Health Organization, "Noncommunicable Diseases," fact sheet, June 1, 2018. As of April 28, 2020: https://www.who.int/news-room/fact-sheets/detail/noncommunicable-diseases

Yang, Tingting, Dan Xie, Zhihong Li, and Hongwei Zhu, "Recent Advances in Wearable Tactile Sensors: Materials, Sensing Mechanisms, and Device Performance," *Materials Science and Engineering: R: Reports*, Vol. 115, 2017, pp. 1–37.

Yu, Kun-Hsing, and Isaac S. Kohane, "Framing the Challenges of Artificial Intelligence in Medicine," *BMJ Quality & Safety*, Vol. 28, 2019, pp. 238–241.

Zaino, Jennifer, "5G vs. 4G Cellular Technology: What Businesses Need to Know," *BizTech*, August 6, 2019. As of April 29, 2020: https://biztechmagazine.com/article/2019/09/5g-vs-4g-cellular-technology-what-businesses-need-know-perfcon

Zhang, Sarah, "People Are Clamoring to Buy Old Insulin Pumps," *The Atlantic*, April 29, 2019. As of July 7, 2020: https://www.theatlantic.com/science/archive/2019/04/looping-created-insulin-pump-underground-market/588091/

Zlotolow, Dan A., and Scott H. Kozin, "Advances in Upper Extremity Prosthetics," *Hand Clinics*, Vol. 28, No. 4, 2012, pp. 587–593.

Zraick, Karen, and Sarah Mervosh, "That Sleep Tracker Could Make Your Insomnia Worse," *New York Times*, June 13, 2019. As of April 29, 2020: https://www.nytimes.com/2019/06/13/health/sleep-tracker-insomnia-orthosomnia.html?module=inline

———, "Public Workshop—Content of Premarket Submissions for Management of Cybersecurity in Medical Devices January 29–30, 2019," webpage, January 2019c. As of April 28, 2020: https://www.fda.gov/medical-devices/workshops-conferences-medical-devices/public-workshop-content-premarket-submissions-management-cybersecurity-medical-devices-january-29-30

U.S. Immigration and Customs Enforcement (ICE), "Law Enforcement Information Sharing Initiative," webpage, U.S. Department of Homeland Security, undated. As of April 28, 2020: https://www.ice.gov/le-information-sharing

Vaas, Lisa, "Doctors Disabled Wireless in Dick Cheney's Pacemaker to Thwart Hacking," *Naked Security*, October 22, 2013. As of April 28, 2020: https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/

Verheij, Robert A., Vasa Curcin, Brendan C. Delaney, and Mark M. McGilchrist, "Possible Sources of Bias in Primary Care Electronic Health Record Data Use and Reuse," *Journal of Medical Internet Research*, Vol. 20, No. 5, 2018, p. e185.

Vermont Public Law H.764 (Act 171), An Act Relating to Data Brokers and Consumer Protection, May 22, 2018. As of April 28, 2020: https://legislature.vermont.gov/bill/status/2018/H.764

Vita-More, Natasha, "Life Extension Leadership Meetings, Conferences, and Festivals," *H Plus Magazine*, July 22, 2018.

Wang, Echo, "China's Kunlun Tech Agrees to U.S. Demand to Sell Grindr Gay Dating App," Reuters, May 13, 2019. As of April 28, 2020: https://www.reuters.com/article/us-grindr-m-a-beijingkunlun/chinas-kunlun-tech-agrees-to-u-s-demand-to-sell-grindr-gay-dating-app-idUSKCN1SJ28N

Waters, Michael, "The Smart Diaper Is Coming. Who Actually Wants It?" *Vox*, May 2, 2019. As of April 28, 2020: https://www.vox.com/the-goods/2019/5/2/18525487/smart-diaper-huggies-monit-pampers-alert-poop-pee

Wee, Sui-Lee, "China Uses DNA to Track Its People, with the Help of American Expertise," *New York Times*, February 21, 2019. As of July 3, 2019: https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html

Whittaker, Zack, "Justice Department Charges Chinese Hacker for 2015 Anthem Breach," *TechCrunch*, May 9, 2019. As of April 28, 2020: https://techcrunch.com/2019/05/09/anthem-breach-indictment

Wicklund, Eric, "FDA Approves mHealth Wearable for Tracking Epileptic Seizures," *mHealth Intelligence*, February 6, 2018. As of April 29, 2020: https://mhealthintelligence.com/news/fda-approves-mhealth-wearable-for-tracking-epileptic-seizures

Wisconsin Statutes §134.98, Notice of Unauthorized Acquisition of Personal Information. As of April 29, 2020: https://docs.legis.wisconsin.gov/statutes/statutes/134/98

Woods, Beau, Andrea Coravos, and Joshua David Corman, "The Case for a Hippocratic Oath for Connected Medical Devices: Viewpoint," *Journal of Medical Internet Research*, Vol. 21, No. 3, 2019. As of July 3, 2019: https://www.jmir.org/2019/3/e12568/pdf

شُكرٌ وعِرفان

إنّ المؤلّفين ممتنّون جداً لجاك دوبوا (Jacques Dubois) لهبته السخيّة لمركز RAND للمخاطر والأمن العالميّ (RAND Center for Global Risk and Security)، التي بفضلها أصبح هذا العمل ممكناً. ويشكر المؤلّفون أيضاً المجلس الاستشاري لمركز RAND للمخاطر والأمن العالميّ (CGRS Advisroy Board)، بالإضافة إلى روبِن ميلي (Robin Meili)، وكينج مالوري (King Mallory)، وكايسي بوسكيل (Casey Bouskill)، لجعْلِهم هذا المشروع ممكناً.

ونودّ أن نشكر كاوليون أوكونيل (Caolionn O'Connell) على تقديم المشورة إلى الفريق وسوني إفرون (Sonni Efron) على مساعدَتها الماهرة في التنقيح. ونودّ أيضاً أن نتوجّه بالشكر إلى مراجعتينا، مارجوري بلومنثال (Marjory Blumenthal)، وهي باحثة أولى في مجال السياسات في مؤسسة RAND، وباتريسيا ستابلِتون (Patricia Stapleton)، وهي عالِمة في مجال العلوم السياسية المقارِنَة والسياسات العامة في مؤسسة RAND، على تعليقاتهما المدروسة حول هذه الدراسة، وريك بين-كروس (Rick Penn-Kraus) على رسومه التوضيحيّة.

ونودّ أيضاً أن نشكر الأشخاص المذكورين فيما يلي على مناقشاتهم ورؤاهم القيِّمة: بيني تشايز (Penny Chase)، جايمس كريستِنسِن (James Christensen)، سيتفِن كريستي (Steven Christey)، آل إموندي (Al Emondi)، أنجيل جوفريا (Angel Giuffria)، أمال جرافسترا (Amal Graafstra)، ماثيو هيبورن (Matthew Hepburn)، تيموثي هانسون (Timothy Hanson)، روبِرت كليتزمان (Robert Klitzman)، وبو وودز (Beau Woods).

وتُنسَب أي أخطاء تَرِد في هذه الدراسة إلى المؤلّفين وحدهم.

عن المؤلّفين

ماري لي (Mary Lee) هي عالِمة رياضيات في مؤسسة RAND وزميلة ساهَمَت في افتتاح مركز RAND للمخاطر والأمن العالميّ (RAND Center for Global Risk and Security). تشمل مجالات اهتمام بحثها النمذجة الرياضيّة ومحاكاة الأنظمة المعقّدة في مجالات الدفاع/الفضاء الجوي، والسياسات الإلكترونية، والرعاية الصحيّة والأمراض المزمنة.

بنجامين بودرو (Benjamin Boudreaux) هو أستاذ في كلية RAND للدراسات العليا (Pardee RAND Graduate school) وباحث في مجال السياسات في مؤسسة RAND، يعمل في مجالات يتقاطَع فيه الأمن القومي، والتكنولوجيا، والأخلاقيات. يركّز بحثه الحالي على القضايا الأخلاقيّة في مجال الذكاء الاصطناعي، وسياسات وسائل التواصل الاجتماعي، والاستجابة للحوادث الإلكترونية.

ريتيكا شاتورفيدي (Ritika Chaturvedi) كانت مهندسة في مؤسسة RAND أثناء إعداد هذا المشروع. إنّها تعمل حالياً بمثابة عالِمة في مجال الأبحاث في مركز شايفر للسياسات الصحيّة وعلْم الاقتصاد (Schaeffer Center for Health Policy and Economics) في جامعة كاليفورنيا الجنوبية (University of South California). تتمتّع بخلفيّة متنوّعة في مجال الهندسة، وسياسات العلوم والتكنولوجيا، وتقييم الأصول، والاستشارات الاستراتيجية، والأبحاث البيولوجية الطبية الناقِلة. إنّها مهتمّة في مسائل العلوم والتكنولوجيا المتعلّقة بالآثار الواسعة النطاق الناجمة عن التكنولوجيات المدمِّرة الناشئة في علوم الحياة والرعاية الصحيّة وعلى المجتمع.

ساشا رومانوسكي (Sasha Romanosky) هو باحث في مجال السياسات في مؤسسة RAND ومستشار سابق في مجال السياسات الإلكترونيّة للبنتاغون في مكتب وزير الدفاع للسياسات (Office of the Secretray of Defense for Policy). تركّز أبحاثه على مواضيع في اقتصاد الأمن والخصوصية، والأمن القومي، وعلْم الاقتصاد الجزئي المُطبَّق، والقانون وعلْم الاقتصاد.

برايس دونينج (Bryce Downing) هو مساعد لشؤون البحث في مؤسسة RAND. قبل الانضمام إلى مؤسسة RAND، كان مُتَدَرِباً في مجال عمليات المحاكاة الاستراتيجية في مركز القيادة الاستراتيجية التابع لكليّة الحرب في الجيش الأمريكي (U.S. Army War College, Center for Strategic Leadership). وتشمل مجالات اهتمام بحثه سياسات التكنولوجيا، ونمذجة عملية صنْع القرارات في ظلّ عدم اليقين، والأمن القومي.

عن هذه الدراسة

لقد أُجري العمل الوارد وصْفه في هذه الدراسة في سياق مشروع زمالةِ من تنظيم مركز RAND للمخاطر والأمن العالميّ (RAND Corporation's Center for Global Risk and Security). وتصف هذه الدراسة التكنولوجيات الناشئة، والتي يُشار إليها هنا بمصطلح إنترنت الأجسام *(Internet of Bodies)*؛ وتحلّل منافعه ومخاطره؛ وتقترح طرقاً يستطيع بها أصحاب الشأن المختلفون تحقيق التوازن بين تلك المنافع والمخاطر. يجب أن تكون هذه الدراسة مهمّةً بالنسبة إلى الرأي العام بالإجمال، ومُصنِّعي أجهزة إنترنت الأجسام والأجهزة الطبية، والجهات المزوِّدة للرعاية الصحية، وصانعي القرارات في السياسات. وقد أُجرِيَ هذا البحث في مركز RAND للمخاطر والأمن العالميّ بين فبراير/ شباط 2019 وسبتمبر/أيلول 2019.

التمويل

لقد تمّ توفير التمويل لهذا المشروع من خلال هبةٍ سخيّة قدّمها جاك دوبوا (Jacques Dubois).

عن مركز RAND للمخاطر والأمن العالميّ (RAND Center for Global Risk and Security)

يعمل مركز RAND للمخاطر والأمن العالميّ (RAND Center for Global Risk and Security) على امتداد مؤسسة RAND لتطوير أبحاثٍ متعددة الاختصاصات وتحليل السياسات التي تتناول المخاطر المنهجية على الأمن العالمي. يعتمد المركز على خبرة مؤسسة RAND لاستكمال أبحاث مؤسسة RAND وتوسيعها في مجالات متعددة، بما في ذلك الأمن، والاقتصاد، والصحة والتكنولوجيا. يقدّم مجلسٌ مؤلّفٌ من كبار قادة الأعمال المتميّزين، والمُحسنين، وصانعي السياسات السابقين المشورة والدعم لأنشطة المركز، التي تركّز بشكلٍ متزايدٍ على اتّجاهات الأمن العالمي وتأثير التكنولوجيات المدمّرة على المخاطر والأمن. لمزيدٍ من المعلومات حول مركز RAND للمخاطر والأمن العالميّ، يرجى زيارة الموقع الإلكتروني www.rand.org/international/cgrs.



للحصول على مزيدٍ من المعلومات حول هذا المنشور، الرجاء زيارة الموقع الإلكتروني: www.rand.org/t/RR3226.



تتوفّر الأجهزة "الذكيّة" المتّصلة بالإنترنت بشكلٍ متزايدٍ في السوق، واعِدةً المُستهلِكين وشركات الأعمال بتحسين الأداء، والملاءمة، والفعاليّة. فضمن نطاق إنترنت الأشياء (Internet of Things [IoT]) هذا الأوسع، تكمن صناعةٌ متناميةٌ لأجهزةٍ تَرْصُد الجسم البشريّ وتنقل عبر الإنترنت البيانات التي يتم جمْعها. يشمل هذا التطوير، الذي أطلق عليه البعض تسمية إنترنت الأجسام (Internet of Bodies [IoB])، مجموعةً متناميةً من الأجهزة التي تجمع البرمجيات، والمعدّات الحاسوبية، وقدرات الاتصالات، من أجل تتبُّع البيانات الصحيّة الشخصيّة، أو توفير العلاج الطبي الحيوي، أو تعزيز راحة الجسد، أو وظيفته، أو صحّته أو رفاهيته. على الرغم من ذلك، تُعقِّد هذه الأجهزة مجالاً محفوفاً أصلاً بالمخاطر القانونية، والتنظيمية، والأخلاقية. فينظر مؤلّفو هذه الدراسة في هذه المجموعة الناشئة من التكنولوجيات المعنيّة بجسم الإنسان والمتصلة بالإنترنت؛ ويستكشف المنافع، والمخاطر من حيث الأمن والخصوصية، والتداعيات الأخلاقية؛ ويجري مسحاً للمشهد التنظيمي الناشئ لهذه الأجهزة والبيانات التي تجمعها؛ ويقدّم توصيات لتحقيق التوازن بين مخاطر إنترنت الأجسام وفوائده.

www.rand.org

Arabic Translation of:
"The Internet of Bodies: Opportunities, Risks, and Governance"
RR-3226/1-RC